Escuela Politécnica Superior

Grupo Universitario de Tecnologías de Identificación (GUTI)

TRABAJO FIN DE GRADO

GRADO EN INGENIERÍA ELECTRÓNICA INDUSTRIAL Y AUTOMÁTICA

EVALUACIÓN DE ACCESIBILIDAD DE SISTEMAS BIOMÉTRICOS EN DISPOSITIVOS MÓVILES

Autor: Álvaro Ludeña Sánchez-Bayuela

Director: Ramón Blanco Gonzalo

Leganés, Octubre 2017

Título: Evaluación de accesibilidad de sistemas biométricos en dispositivos móviles

Autor: Alvaro Ludeña Sánchez-Bayuela

Director: Ramón Blanco Gonzalo

EL TRIBUNAL

Presidente: Pedro Martín Mateos

Vocal: Juan Miguel García Haro

Secretario: Ignacio Rubio Díaz

Realizado el acto de defensa y lectura del Trabajo Fin de Grado el día 10 de octubre de 2017 en la Escuela Politécnica Superior de la Universidad Carlos III de Madrid. Se acuerda otorgar la CALIFICACIÓN de

Firma: Presidente Firma: Vocal Firma: Secretario

Agradecimientos

En este punto voy a intentar acordarme de todas las personas que, de forma directa o indirecta, han confiado en mí durante mi trayectoria académica, ayudándome a llegar hasta aquí.

En primer lugar, agradecer al GUTI (Grupo Universitario de Tecnologías de Identificación) su ayuda y su apoyo para realizar el presente proyecto. Mención especial a Ramón Blanco, quién me ha acompañado a lo largo de todo el proceso, ofreciendo su ayuda y apoyo ante cualquier circunstancia de forma incondicional.

También me quiero acordar de Carlos Sánchez Redondo, cuya ayuda fue primordial para desarrollar la aplicación móvil que se evalúa en este trabajo, a pesar de que por circunstancias tuvo que abandonar el GUTI un mes después de que yo llegara.

Por otro lado, debo mencionar a Chiara Lunerti, estudiante italiana que estuvo durante unos meses de intercambio con la universidad y, al ver en qué consistía nuestro proyecto, se volcó de lleno para ayudar en lo que fuera. Gracias Chiara por compartir tu experiencia en el ámbito de la biometría y por ayudarme a lo largo de estos meses.

Me quiero acordar también de todas las personas que me han apoyado desde que me embarqué en esta etapa universitaria. Desde el principio tuve la suerte de entrar en un grupo de amigos formado por Víctor Jiménez, Fernando Landrove, Alejandro Mancheño, Jesús Olivares, Joaquín Peinado. Chicos, muchas gracias por estar en las malas y en las buenas. Hemos sufrido juntos cada tropiezo, pero sobretodo, ¡Hemos celebrado cada logro!

Quiero agradecer, de todo corazón, el gran esfuerzo que han hecho y siguen haciendo mis padres para brindarme la oportunidad de formarme tanto a nivel de estudios como a nivel personal. Gracias por empujarme y por estar siempre a mi lado, aguantando mi mal humor cuando las cosas no salían bien y animándome a seguir adelante. Gracias también a mi hermana pequeña, María Isabel Ludeña, con la que tantas veces me he desahogado tirando unas canastas o chinchándola cuando me invadía el aburrimiento o el estrés tras tirarme horas y días leyendo apuntes.

Finalmente quiero dar mil gracias a toda la gente que ha participado en mi TFG de forma desinteresada, tanto a la gente del CRMF [1] (Centro de Recuperación de personas con Discapacidad Física) como a gente que no pertenece al CRMF (gente perteneciente al Colegio Mayor Fernando Abril Martorell, y mis familiares y amigos del trabajo). Sin vosotros este proyecto no habría sido posible.

Índice

Capítulo 4:

Capítulo 5:

Índice de Figuras

Índice de Tablas

Capítulo 1

Introducción y objetivos

En este capítulo se realizará una breve introducción del proyecto, se expondrán las motivaciones, los objetivos que nos planteamos y se dará una visión general del presente documento.

1.1. Introducción

Actualmente, la tecnología se encuentra presente ante la mayoría de situaciones que vivimos en nuestra vida cotidiana, ya sea llamar por teléfono, sacar dinero de un cajero, realizar compras por internet, sacar el ticket para el autobús, tren o metro, pero, ¿Estamos seguros de si estas tecnologías son cien por cien seguras?

Los sistemas biométricos en conjunto con la tecnología Smartphone están sufriendo un gran desarrollo desde hace tiempo. Sentirse protegido y seguro mientras usamos nuestro teléfono móvil, es uno de los principales objetivos que se intentan alcanzar en esta era de revolución digital y la biometría está consiguiendo alcanzar estas metas con creces.

En definitiva, uniendo tecnología Smartphone con biometría, se puede intentar ayudar a mejorar la calidad de vida de personas, especialmente la de aquellas con problemas de accesibilidad. Esta es la idea principal en torno a la cual se desarrolla nuestro proyecto.

Haciendo uso de una aplicación móvil desarrollada por el GUTI [2] , se pedirá a los usuarios que se autentiquen ellos mismos para retirar dinero de un cajero automático ficticio (representado por un tablet PC) habiendo realizado un reclutamiento previo. La autenticación se realizará a través de modalidades biométricas y no biométricas, con la finalidad de realizar una evaluación de accesibilidad, de tal forma que comprobaremos si el uso de la biometría es útil, soluciona problemas y además se estudiará la forma de implementar mejoras.

1.2. Motivación

Hace un año cursé en Alemania la asignatura "*Automotive System Evaluation*". Para finalizar dicha asignatura, se tuvo que realizar un experimento cuyo objetivo era comprobar si el riesgo era mayor cuando se conduce mientras se envía un mensaje de texto haciendo uso de un teléfono móvil táctil o con un teléfono con teclado. Para ello se usó un programa de ordenador que simulaba una carretera en la cual circulaba un coche que era manejado por el usuario a través de un volante y unos pedales conectados con el programa. El usuario haría uso de este programa al mismo tiempo que enviaba un mensaje con un teléfono móvil táctil y después con un teléfono móvil con teclas.

Tras esta primera toma de contacto con este tipo de estudios, la idea de poder ayudar y facilitar la vida a las personas mediante el uso de tecnología me resulta fascinante.

Actualmente el uso de biometría en los teléfonos móviles está en auge. Todo dispositivo móvil que sale al mercado lleva incorporada alguna novedad con respecto a esta tecnología. Según un estudio realizado por la plataforma *Online Back Market*, *"el 92% de españoles tiene al menos un dispositivo móvil inteligente"* [3], dando lugar a que

el conjunto de Smartphone y biometría abra un gran abanico de posibilidades. Por ejemplo, cada día son más los bancos o aplicaciones de compra online que ofrecen la posibilidad de efectuar pagos a través de la cuenta bancaria del usuario, haciendo uso de su huella dactilar como método de seguridad.

Otra posibilidad, la cual es nuestro objeto de estudio, sería ayudar a personas con problemas de accesibilidad a retirar dinero de un cajero. Hoy en día, la mayoría de personas tiene una o varias cuentas en distintas entidades bancarias, cada una con un número secreto distinto que debemos recordar. Si a este número le añadimos también las claves que debemos recordar para abrir nuestro correo, nuestra cuenta de ordenador, nuestra cuenta de la universidad y un largo etcétera de situaciones parecidas, es totalmente lógico que muchas de las contraseñas se nos olviden. Esta situación puede remediarse gracias al uso de la biometría, que brinda una forma segura de reconocer y autenticar la identidad del usuario sin necesidad de tener que memorizar claves.

1.3. Objetivos

Este proyecto tiene varios propósitos cuya finalidad es contribuir a la mejora de la accesibilidad y usabilidad de los sistemas de reconocimiento biométrico.

Podemos definir varios objetivos fundamentales:

- Estudiar la accesibilidad y usabilidad del sistema de retirada de dinero que se ha desarrollado para los usuarios tanto del CRMF como los ajenos al centro.
- Comparar mecanismos de autenticación tradicional con mecanismos biométricos en términos de rendimiento, usabilidad y accesibilidad.
- Estudiar la accesibilidad de las modalidades de autenticación biométrica más comunes en los dispositivos móviles.
- A partir del estudio, conocer los requisitos de accesibilidad que debe cumplir una aplicación de estas características.
- Encontrar mejoraras que puedan ser implementadas en esta u otras futuras aplicaciones móviles, con la finalidad de conseguir que cualquier usuario tenga las mismas oportunidades a la hora de usar un cajero automático o realizar una transferencia bancaria.

1.4. Contenido del proyecto

La presente memoria sigue la siguiente estructura:

En primer lugar, tras haber realizado una breve introducción al campo que se va a estudiar, se definirán varios conceptos importantes a los que nos referiremos de forma continua a lo largo del proyecto. Estos conceptos son, biometría, reconocimiento biométrico, autentificación e identificación. Además, se realizará un breve resumen de la historia de la biometría, para que el lector tenga una visión general de la evolución que esta tecnología ha sufrido a lo largo del tiempo hasta nuestros días.

También se deben definir dos términos de vital importancia, ya que en ellos vamos a basar los resultados y las conclusiones que obtengamos a lo largo de la evaluación. Estos términos son usabilidad y accesibilidad.

Una vez explicada toda la terminología, se procederá a explicar el diseño de la evaluación, describiendo el experimento en detalle, analizando todos los pasos que han seguido los usuarios, así como el hardware y software usado. Se expondrá también toda la documentación necesaria para que los usuarios puedan participar en la evaluación, así como los formularios que los usuarios que participan en la evaluación deben rellenar para registrar su opinión sobre la tecnología que se va a usar antes y después de haber entrado en contacto con ella durante el experimento.

Una vez explicado el proceso que los usuarios han seguido, se expondrán los resultados obtenidos (rendimiento, usabilidad y accesibilidad).

Finalmente se sacarán conclusiones de los resultados expuestos y se realizará una guía de buenas conductas que ofrecerá mejoras que se pueden llevar a cabo en futuros experimentos.

Al final de documento podremos encontrar un presupuesto sobre la evaluación realizada, así como anexos sobre los documentos que los usuarios deben firmar antes de participar en la evaluación y cuestionarios que dichos usuarios deben rellenar antes y después de la evaluación para aportar sus opiniones sobre las pruebas realizadas.

Capítulo 2

Estado del arte

En este capítulo, en primer lugar, se explicarán los conceptos de biometría y reconocimiento biométrico. Posteriormente, se realizará un breve resumen de la historia de la biometría hasta la actualidad. También se definirán dos conceptos importantes, autenticación e identificación.

Por otro lado, se dará una visión general de la arquitectura de un sistema de reconocimiento biométrico y se hablará de la situación de la biometría en la actualidad.

Finalmente definiremos los conceptos de usabilidad y accesibilidad.

2.1. Biometría y reconocimiento biométrico

2.1.1. Biometría

"*La biometría es la ciencia que estudia la identidad de un individuo basándose en sus atributos físicos, químicos o de comportamiento de la persona*" [4]. En otras palabras, "*la biometría es la ciencia dedicada a medir y analizar características del cuerpo humano tales como el ADN, las huellas dactilares, la retina y el iris de los ojos, los patrones faciales, los patrones de la voz, la geometría o las venas de la mano"* [5].

Cada atributo biométrico tiene sus ventajas y desventajas, por lo que la elección de un rasgo biométrico para una aplicación determinada, depende de una variedad de factores, entre los cuales podemos destacar los siguientes [4]:

1. **Universalidad.** Cada individuo que accede a la aplicación debe contener el rasgo.

2. **Unicidad.** El rasgo que se quiera analizar debe ser suficientemente diferente entre los individuos que componen la población.

3. **Permanencia.** El rasgo biométrico de un individuo debe ser suficientemente invariante a lo largo de un período de tiempo con respecto al algoritmo de coincidencia. Un rasgo que cambia significativamente con el tiempo no es un rasgo biométrico útil.

4. **Mensurabilidad.** Debería ser posible adquirir y digitalizar el rasgo biométrico utilizando dispositivos adecuados que no causen inconvenientes indebidos al individuo. Además, los datos brutos adquiridos deben ser susceptibles de procesamiento para extraer conjuntos de características representativas.

5. **Rendimiento.** La precisión de reconocimiento y los recursos necesarios para lograr dicha precisión deben cumplir con las restricciones impuestas por la aplicación.

6. **Aceptabilidad.** Los individuos de la población objetivo que utilizarán la aplicación deberán estar dispuestos a presentar su rasgo biométrico al sistema.

7. **Fiabilidad.** Facilidad con la que el rasgo de un individuo puede ser imitado usando artefactos, por ejemplo, dedos falsos en el caso de rasgos físicos, o, mimetismo en el caso de rasgos conductuales.

Basándonos en estas características debemos decidir si aceptar o no rasgos físicos o de comportamiento como características biométricas.

2.1.2. Reconocimiento biométrico

Entenderemos por reconocimiento biométrico al método basado en biometría, cuya finalidad es identificar y autenticar la identidad de un individuo de forma automática a través de sus rasgos físicos y de comportamiento.

Según se observa en la Figura 1, podremos clasificar el reconocimiento biométrico en dos grupos, rasgos físicos y rasgos de comportamiento:

- **Reconocimiento de rasgos físicos:** huellas dactilares, geometría del iris, geometría de las manos y geometría de cara entre otros.

- **Reconocimiento de rasgos de comportamiento:** firma manuscrita, dinámica de pulsación de teclas, así como la dinámica de pasos que realizamos al andar entre otros.

La voz se considera una mezcla de características dinámicas y físicas.

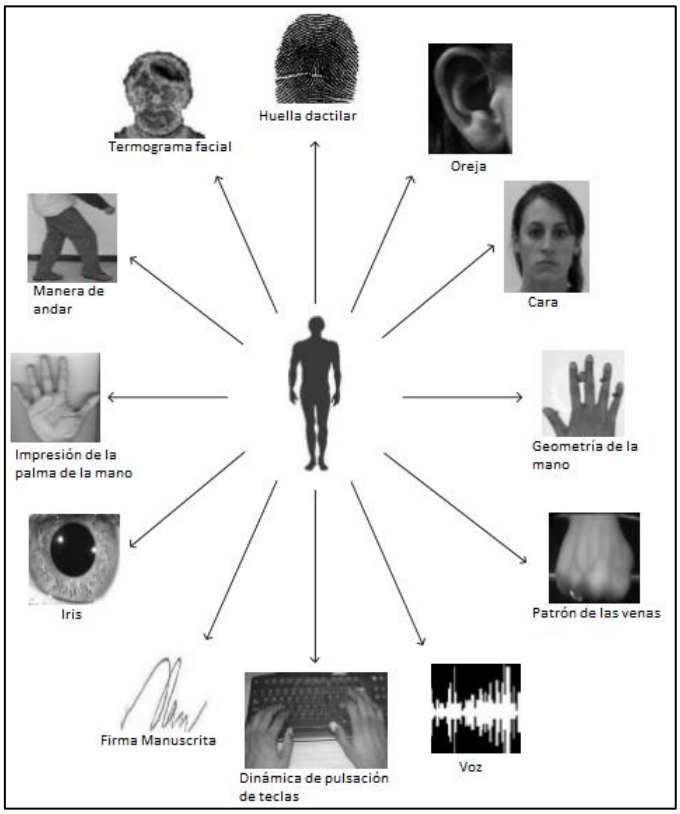

Figura 1. Ejemplo de rasgos que pueden usarse para realizar reconocimiento biométrico [4]

2.2. Historia de la biometría

El reconocimiento biométrico se basa en diferenciar a individuos a través de características especiales. Los humanos siempre se han identificado entre ellos a través de las caras, la voz o la forma de caminar entre otras características. Son muchas las evidencias que hay en la historia sobre el uso de la biometría [4].

Los primeros antecedentes de los cuales se tiene constancia sobre el uso de la biometría datan del siglo XIV en China. El escritor y explorador Joao Barros escribió que los comerciantes chinos usaban las huellas de las manos de los niños en un papel con tinta con la finalidad de distinguir entre niños y jóvenes.

La biometría no se puso en práctica en las culturas occidentales hasta finales del siglo XIX. En esta época la identificación de individuos era confiada a la memoria fotográfica, hasta que, en 1883, Alphonse Bertillon, antropólogo que trabajó como jefe de departamento fotográfico de la Policía de Paris, desarrolló el sistema antropométrico, más conocido como "Bertillonage" [6]. Este era el primer sistema preciso y ampliamente utilizado científicamente para identificar a criminales y convirtió a la biometría en un campo de estudio.

Tal y como se puede apreciar en la Figura 2, el sistema de Bertillon funcionaba midiendo de forma precisa ciertas longitudes y anchuras de la cabeza y del cuerpo, así como registrando marcas individuales como tatuajes y cicatrices.

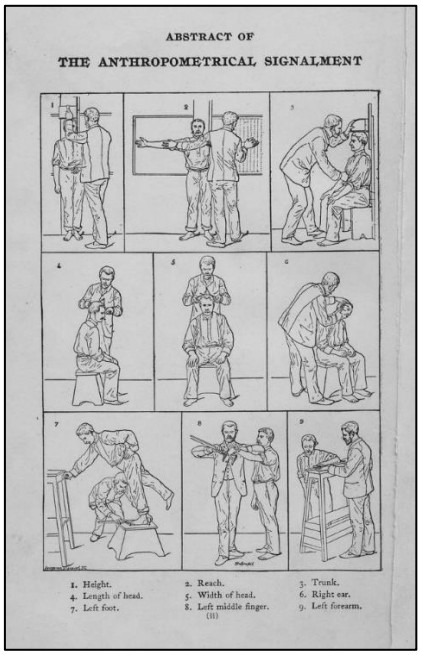

Figura 2. Sistema de Bertillon [6]

El sistema de Bertillon fue adoptado extensamente en occidente hasta que aparecieron defectos en el sistema como, por ejemplo, dificultades para diferenciar sujetos extremadamente similares, como sucedía con individuos gemelos.

Tras la desacreditación que sufrió el sistema de Bertillon, se comenzó a buscar otros métodos de identificación biométrica. Es entonces cuando las investigaciones de Sir Francis Galton sobre el uso de la huella dactilar cobran una gran importancia, siendo rápidamente aceptadas por toda la comunidad a nivel mundial.

El uso práctico de huellas dactilares como método de identificación de individuos ha sido utilizado desde finales del siglo XIX cuando Sir Francis Galton definió algunos de los puntos o características desde las cuales las huellas dactilares podían ser identificadas [7]. Estos "puntos Galton" son la base para la ciencia de identificación por huella dactilar, la cual se ha expandido y ha sufrido una transición en el pasado siglo.

La identificación por huella digital comienza su transición a la automatización a finales de los años 60 junto con la aparición de las tecnologías de computación. Con la llegada de las computadoras, un subconjunto de los puntos Galton, ha sido utilizado para desarrollar la tecnología de reconocimiento automatizado de huellas dactilares. En 1969, hubo un empuje mayor por parte del "*Buró Federal de Investigaciones*" (FBI) para desarrollar un sistema para automatizar sus procesos de identificación por huellas dactilares, el cual rápidamente se había vuelto abrumador y requería de muchas horas hombre para el proceso manual. El FBI contrató al Buró Nacional de Estándares (NBS), ahora Instituto Nacional de Estándares y Tecnología (NIST), para estudiar el proceso de automatización de la clasificación, búsqueda y concordancia de la huella dactilar [8].

A finales de 1990, los algoritmos de reconocimiento biométrico mejoraron notablemente, gracias a los trabajos realizados por el FBI y el NIST, quienes se involucraron de lleno en la biometría forense creando en 1998 una base de datos de ADN, así como organizando evaluaciones biométricas como, por ejemplo, el Procedimiento de Evaluación del Reconocimiento Facial (FERET) en 1993 [9] o la evaluación del Sistema Integrado Automatizado de Identificación de Huellas Dactilares (IAFIS) en 1994.

A día de hoy, se ha investigado y se sigue investigando mucho en el campo de la biometría, detectándose multitud de rasgos biométricos diferentes a la huella dactilar. El avance en el conocimiento de dichos rasgos y sus correspondientes ventajas e inconvenientes, unido a las posibilidades que ofrece la tecnología, hacen que la biometría se considere uno de los elementos clave en cuanto a las técnicas de identificación y seguridad en el futuro.

2.3. Autenticación vs identificación

Hay que distinguir entre autenticación y verificación ya que son términos con significados distintos [10]:

- **Autenticación.** Proceso a través del cual los rasgos biométricos se comparan solamente con los de un patrón ya guardado. Este proceso implica conocer presuntamente la identidad del individuo a autenticar, por lo tanto, dicho individuo ha presentado algún tipo de credencial que después del proceso de autenticación biométrica será validada o no.

- **Identificación.** Proceso a través del cual los rasgos biométricos se comparan con lo de un conjunto de patrones ya guardados. Este proceso implica no conocer la presunta identidad del individuo, ya que la muestra de datos biométricos es tomada del usuario y comprobada una a una con los patrones ya existentes en el banco de datos registrados.

En definitiva, el resultado del proceso de identificación es conocer la identidad del individuo mientras que en el proceso de autenticación el resultado es obtener un valor de verdadero o falso.

2.4. Clasificación de sistemas biométricos [11]

Se entiende por sistema biométrico al método automático para el reconocimiento único de individuos basado en rasgos conductuales o físicos. Dependiendo del tipo de característica que se vaya a utilizar para llevar a cabo el reconocimiento biométrico, podemos dividir las modalidades biométricas en dos grupos [11]:

- **Estática.** Biometría que mide las características físicas de un individuo. Los principales estudios que podemos encontrar en este grupo son aquellos basados en: huellas dactilares, geometría de la mano, análisis de iris y retina y reconocimiento facial.

- **Dinámica.** Biometría que mide los rasgos de comportamiento de un individuo. Los principales estudios que podemos encontrar en este grupo son aquellos basados en: firma manuscrita o la forma de caminar entre otras.

Tal y como se ha mencionado en el punto anterior, la voz es una mezcla de biometría dinámica y estática.

2.5. Arquitectura y funcionamiento de los sistemas biométricos

Podemos dividir el funcionamiento de los sistemas biométricos en varias fases, tal y como se puede apreciar en la Figura 3. En base a la aplicación que se desee diseñar, se deberá completar todas las fases o un subconjunto de ellas [12]:

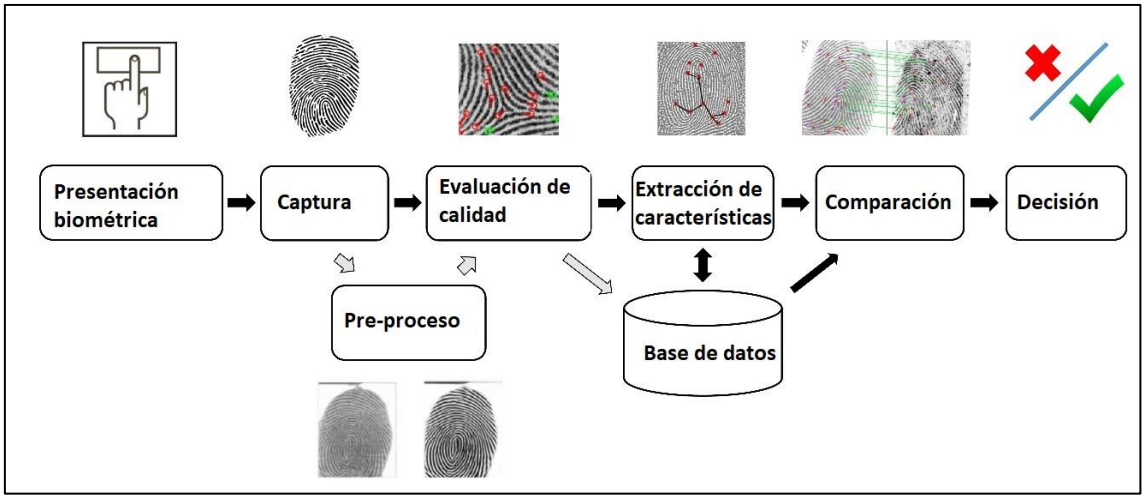

Figura 3. Fases generales de un proceso de reconocimiento biométrico.

- **Presentación biométrica.** El sistema biométrico adquiere, de forma digital o analógica, un indicador biométrico del individuo (muestra). Factores como el ambiente o la interacción hombre-computadora (HCI) cobran gran importancia en la calidad de la muestra.

- **Captura.** La captura es realizada por un sistema capaz de detectar rasgos biométricos. En algunos casos, el sistema no detecta el rasgo biométrico, sino que simplemente captura de forma manual o automática la información (por ejemplo, esto sucede con la toma de fotografías o una grabación de audio).

- **Pre-procesamiento.** En esta fase, se mejora la calidad de la muestra tomada, adaptando la muestra a los requerimientos de entrada de algoritmo. Esta fase no es obligatoria, pero si se recomienda con la finalidad de mejorar el rendimiento del algoritmo.

- **Evaluación de calidad.** Una vez capturado el rasgo biométrico, la muestra puede ser o no suficiente para ser procesada. Para comprobar la calidad de dicha muestra, algunos sistemas incorporan evaluaciones de calidad, por lo que, si la muestra está por debajo de un umbral dado, el sujeto debe presentar de nuevo el rasgo biométrico.

- **Extracción de características.** En esta fase, el sistema extrae características del rasgo biométrico que se ha introducido (a esto se le denominara vector de características). Este proceso es necesario para hacer coincidir las muestras (que coinciden con las características) y reduce el espacio requerido en la base de datos si el sistema solo almacena los vectores de características.

- **Comparación.** En esta fase se realiza una comparación entre dos muestras, devolviendo la probabilidad de coincidencia entre ellas. Cuanto mayor sea esta probabilidad, mayor es la certeza de que ambas muestras pertenezcan al mismo sujeto.

- **Decisión.** En esta fase se decide si el usuario es genuino o un impostor, basándose en el resultado obtenido durante la comparación. Si la probabilidad está por encima de un umbral prefijado, el reconocimiento sería correcto. En caso contrario, el sujeto no será reconocido.

Podemos resumir la arquitectura de nuestra evaluación en dos módulos que incorporan todas las fases que se acaban de explicar: módulo de reclutamiento y módulo de reconocimiento.

A continuación, se explica como de desarrollan ambos módulos.

2.5.1. Módulo de reclutamiento [13]

Este módulo se encarga de adquirir y almacenar la información proveniente del indicador biométrico del individuo, con el objetivo de poder contrastar la información con la que será proporcionada en ingresos posteriores del sistema. Las labores ejecutadas por el módulo de inscripción son posibles gracias a la acción del lector biométrico y del extractor de características. El primero se encarga de adquirir datos relativos del indicador biométrico elegido y entregar una representación en formato digital de éstos. El segundo extrae, a partir de la salida del lector, características representativas del indicador.

Durante este proceso de recopilación de datos aparecen los primeros problemas. En primer lugar, las muestras deben ser obtenidas mediante un sensor, por lo tanto, están sujetas a la calidad y características técnicas del sensor utilizado, lo que obliga a que las características del sensor deberán ser estandarizadas, a fin de garantizar que las muestras obtenidas de un usuario en diferentes sistemas sean compatibles. En cuanto al almacenamiento, existen varias formas de guardar los datos previamente recopilados y procesados, que al momento de ser almacenados reciben el nombre de patrón.

El conjunto de procesos realizados por el módulo de inscripción recibe el nombre de fase de inscripción.

2.5.2. Módulo de reconocimiento

Este módulo se encarga de la identificación de individuos. El proceso de identificación comienza cuando el lector biométrico captura la característica del individuo a ser identificado y la convierte a formato digital siempre que la muestra supere un umbral fijado con la finalidad de que la muestra sea de una calidad suficiente (pre-procesado) para que, a continuación, el extractor de características produzca una representación compacta con el mismo formato que el del patrón.

El conjunto de procesos realizados por el módulo de reconocimiento recibe el nombre de fase operacional.

2.6. Biometría en la actualidad

Desde hace años, la biometría ha adquirido un papel importante en numerosos ámbitos en cuanto a seguridad se refiere. Actualmente, la biometría está intentando posicionarse como un método de seguridad fiable y cómodo de usar en dispositivos móviles, tratando de permitir un acceso rápido al dispositivo, sin necesidad de recordar contraseñas ni códigos.

La biometría puede aplicarse en una amplia variedad de contextos, por ejemplo, los usuarios pueden autenticarse en una aplicación de banca móvil utilizando una o una combinación de diferentes modalidades biométricas, como reconocimiento facial y de voz, para que puedan realizar pagos seguros o transferencias directas desde sus teléfonos inteligentes.

La biometría está reemplazando los mecanismos de autenticación convencionales como el PIN o la contraseña gráfica como patrón para desbloquear la pantalla del dispositivo, o puede usarse como una combinación de ellos para hacer aún más segura la protección de datos confidenciales importantes, como puede ser el acceso a una cuenta bancaria.

Habitualmente, la presentación de la característica biométrica que se vaya a usar es fácil, por ejemplo, en el caso de reconocimiento dactilar, tan solo basta con colocar nuestro dedo sobre un sensor incorporado en el dispositivo móvil, para verificar nuestra identidad al instante. En otras ocasiones, este proceso puede ser incluso automático, sin que el usuario realice ninguna acción, como sucede por ejemplo en el reconocimiento facial, donde el usuario simplemente mira a la pantalla del móvil y la aplicación móvil le reconoce el rostro rápidamente sin necesidad de pulsar ningún botón.

Sin embargo, el uso de la biometría cuenta con una serie de impedimentos que no permiten que esta tecnología se expanda más rápido. Existe un gran número de personas que tienen miedo a lo desconocido y prefieren seguir haciendo uso de métodos de seguridad tradicionales como el uso de PIN. Muchas veces, existe preocupación acerca del robo de identidad por el uso de la biometría, ya que, si nuestros

datos biométricos son robados, los daños son irreversibles, cualquiera que posea nuestros datos biométricos podrá suplantar nuestra identidad de por vida. Por otro lado, la expansión de la biometría se ve frenada por el alto coste que conlleva la tecnología necesaria.

A pesar de estos inconvenientes, cada día la biometría va siendo más conocida y usada por un mayor número de personas gracias a los nuevos avances que el sector de telefonía móvil va incorporando en sus nuevos modelos. Además, la comodidad que esta tecnología ofrece en conjunto con la creciente mejora en la privacidad y seguridad que se realiza de forma continuada sobre este campo, hace que la biometría tenga asegurado su futuro.

2.7. Sistemas no biométricos. Pin y patrón de seguridad

Como se ha comentado en el punto anterior, hay personas que se encuentran más cómodas usando métodos tradicionales frente al uso de la biometría para identificarse. Básicamente estos métodos se reducen al uso de un código pin o de un patrón de seguridad.

En el presente proyecto estos métodos de identificación también son usados con la finalidad de conocer la opinión de los usuarios tras haber usado tanto métodos tradicionales como métodos biométricos para identificarse. Por ello, se va a dar una breve explicación de cada uno de ellos.

2.7.1. Uso de Pin

El uso de un código pin como método de seguridad, es uno de los más antiguos que existen. En este proyecto se va usar un código pin formado por 4 dígitos, tal y como se puede apreciar en la Figura 4. Es un método fácil y seguro de usar siempre y cuando se recuerden los números seleccionados.

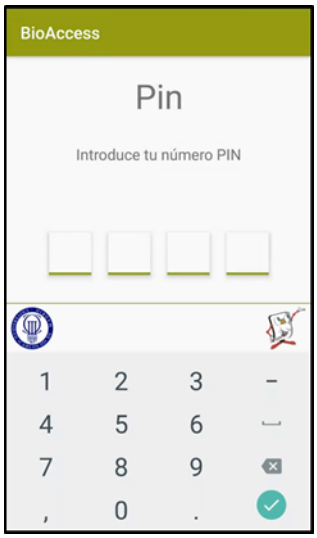

Figura 4. Ejemplo de interfaz del código pin

2.7.2. Uso de patrón de seguridad

Tal y como podemos ver en la Figura 5, este método de seguridad consiste en una matriz de nueve puntos donde se puede dibujar un recorrido entre algunos o todos estos puntos, sin retirar el dedo de la superficie de la pantalla.

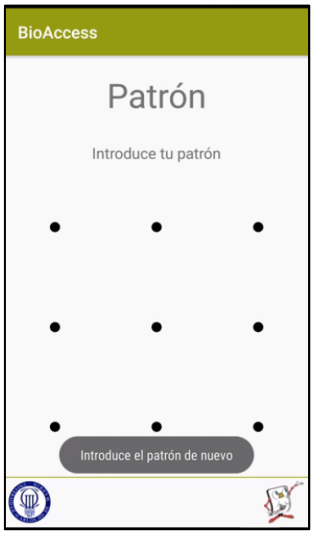

Figura 5. Ejemplo de interfaz del patrón de seguridad

2.8. Usabilidad y accesibilidad

A continuación, vamos a definir los conceptos de usabilidad y accesibilidad, términos fundamentales en los cuales nos hemos basado para realizar nuestro proyecto y sacar conclusiones sobre ellos.

2.8.1. Usabilidad

Haciendo referencia a la norma ISO 9241-11:1998 "Guidance on usability", el término usabilidad se define como "*la medida con la que un producto se puede usar por usuarios determinados para conseguir objetivos específicos con efectividad, eficiencia y satisfacción en un contexto de uso concreto*" [14].

En definitiva, para medir la usabilidad de un producto se tienen en cuenta los siguientes aspectos [14]:

- **Efectividad** Exactitud e integridad con la que los usuarios alcanzan los objetivos especificados, y por consiguiente implica facilidad de aprendizaje, ausencia de errores del sistema o facilidad de dicho sistema para ser recordado. Para medir la efectividad se tendrá en cuenta:

  -Número de tareas importantes realizadas.

  -Porcentaje de funciones relevantes utilizadas.

  -Porcentaje de tareas completadas con éxito al primer intento.

  -Número de referencias a la documentación.

  -Número de acceso a la ayuda.

  -Porcentaje de usuarios capaces de aprender sus características.

  -Porcentaje de errores corregidos o reportados por el sistema.

  -Número de errores de los usuarios tolerados.

- **Eficiencia.** Recursos empleados (esfuerzo, tiempo, etc.) en relación con la exactitud e integridad con la que los usuarios alcanzan los objetivos especificados. Las métricas definidas son:

  -Eficiencia relativa en comparación con un usuario experto.

-Tiempo empleado en el primer intento.

-Tiempo empleado en reaprender funciones.

-Número de errores persistentes.

-Tiempo productivo.

-Tiempo para aprender características.

-Tiempo para reaprender características.

-Eficiencia relativa durante el aprendizaje.

-Tiempo empleado en la corrección de errores.

- **Satisfacción.** Factor subjetivo que implica una actitud positiva en el uso del producto. Las métricas definidas son:

  -Calificación, por parte del usuario, de su satisfacción con las características importantes.

  -Tasa de uso voluntario del producto.

  -Frecuencia de reutilización del producto.

  -Calificación, por parte del usuario, de la facilidad de aprendizaje.

  -Calificación, por parte del usuario, del tratamiento de errores.

2.8.2. Accesibilidad

Haciendo referencia a la norma ISO 26800:2011 "Ergonoics-General approach, principles and concepts" se define accesibilidad como *"el grado en que productos, servicios, entornos e instalaciones, pueden ser usados por personas de una población con el más amplio rango de características y capacidades, para lograr un objetivo determinado en un contexto específico de uso*" [15]

La accesibilidad es un término indispensable e imprescindible, ya que se trata de una condición necesaria para que cualquier persona, independientemente de las posibles limitaciones funcionales que pueda tener, goce de las mismas oportunidades dentro de lo posible, a la hora de utilizar un objeto, visitar un lugar o acceder a un servicio.

Aún queda mucho por mejorar en este ámbito, pero, a día de hoy son muchos los sectores que han realizado grandes avances en cuanto a accesibilidad se refiere como por ejemplo los sectores de la medicina, el transporte o la informática, facilitando la vida a personas con algún tipo de discapacidad o limitación funcional.

Desde hace unos años, en el sector de las TIC (Tecnología de la Información y la Comunicación) se han publicado numerosas medidas para evaluar la accesibilidad en este ámbito. Dichas medidas se encuentran recogidas en la norma europea EN 301 549 V1.1.2 – 2015- "Accessibility requirements suitable for public procurement of ICT products and services in Europe". [16]

Capítulo 3

Diseño del experimento

En este capítulo describiremos en que va a consistir nuestro experimento, el diseño del proyecto y los datos que se van a recoger a lo largo de la evaluación.

3.1. Descripción del experimento

Nuestro experimento consiste en evaluar la accesibilidad y usabilidad de una aplicación instalada en un teléfono móvil inteligente, basada en la retirada de dinero de un cajero automático ficticio, el cual es simulado a través de una tablet. La aplicación móvil se crea bajo el nombre de "*Bioaccess*" la cual, como se ha mencionado en puntos anteriores, ha sido desarrollada por él GUTI [2].

Para lograr esta retirada de dinero del cajero, el usuario debe realizar una serie de pasos previos para identificarse como propietario de la cuenta a la que se está intentando acceder. Con la finalidad de lograr esta identificación se van a usar métodos tradicionales, como el uso de un código pin y un patrón de seguridad, así como métodos más novedosos, como es el uso de la biometría: huella dactilar, reconocimiento de voz y reconocimiento facial.

En el experimento participan tanto personas pertenecientes al CRMF como personas ajenas a este centro, que pueden tener o no problemas de accesibilidad. La participación de todos los usuarios es totalmente voluntaria.

3.2. Diseño de la evaluación

La evaluación se ha diseñado de acuerdo a la norma ISO/IEC 19795-2:2007 "Testing *methodologies for technology and scenario evaluation*" [17] así como la metodología desarrollada por Fernandez-Saavedra [18].

Solo se plantea un escenario en la evaluación debido a las siguientes razones:

- Los usuarios deben intentar en todo momento realizar las tareas por si solos en la medida de lo posible, por lo que, si se planteara más de un escenario, sería más complicada que los usuarios recordaran los pasos a seguir, pudiendo confundir escenarios. Además, es necesario plantear un escenario donde el usuario pueda estar tranquilo debido a sus características.

El escenario elegido para realizar la evaluación simula un punto de retirada de dinero representado por una tablet (cajero automático) y un teléfono móvil inteligente, situados sobre una mesa dentro de una habitación donde no haya ruido de fondo, donde las paredes sean blancas sin ningún tipo de cuadro o fondo desigual, y donde la luminosidad sea buena. Los dispositivos mencionados se dispondrán de acuerdo a las preferencias de usuario, siempre que pueda interactuar con ellos sin dificultad.

Evaluaremos a dos grupos de usuarios con distintas características, usuarios pertenecientes al CRMF [1] y usuarios ajenos al CRMF que no tienen problemas de accesibilidad. De esta forma, podremos analizar los datos de cada grupo por separado y sacar conclusiones más concretas sobre la accesibilidad y usabilidad de nuestra aplicación.

Capítulo 4

Desarrollo del experimento

En este capítulo se explicará, de forma detallada, todos los pasos que se han seguido a lo largo de la evaluación. También se hará una descripción del software y del hardware usado. Por último, se detallarán los documentos de aceptación que los usuarios deben firmar antes de realizar la evaluación y los formularios que los usuarios debían responder tras realizar las distintas fases del experimento.

4.1. Metodología y recogida de datos

En primer lugar, una vez verificado el correcto funcionamiento de la aplicación móvil, la cual es proporcionada por el GUTI, se buscan usuarios que quieran participar de forma voluntaria en nuestra evaluación.

Gracias a estudios hechos en años anteriores, recurrimos al CRMF quien acepta participar.

Cada usuario que participe en la evaluación deberá acudir a dos sesiones que tendrán lugar en dos días distintos, dejando pasar como mínimo una semana entre ambos días. El tiempo estimado de cada sesión es de unos 10 o 15 minutos dependiendo del usuario. Esta estructura de evaluación se ha desarrollado de acuerdo a la ISO/IEC 19795-1:2006 "*Biometric performance testing and reporting — Part 1: Principles and framework*" [19].

La totalidad de la evaluación se divide en dos sesiones:

- **Sesión 1.** Tal y como se puede apreciar en la Figura 6, durante el primer día el usuario realizará las siguientes tareas:

  - **Reclutamiento.** El usuario firma el documento de conformidad donde acepta participar en la evaluación y rellena un breve formulario inicial. Posteriormente se da una breve explicación de cómo funciona la aplicación móvil que va a usar y se recogen en la base de datos la información biométrica, pin y patrón que el usuario usará para identificarse en la aplicación móvil a la hora de retirar dinero del cajero automático. En esta etapa se asistirá al usuario en todo lo necesario, respondiendo todas sus dudas acerca del uso de la aplicación móvil.

  - **Verificación 1.** Tras realizar el reclutamiento, el usuario realiza la primera visita al cajero. En esta etapa se ayudará al usuario cuando lo requiera. El examinador intervendrá lo menos posible.

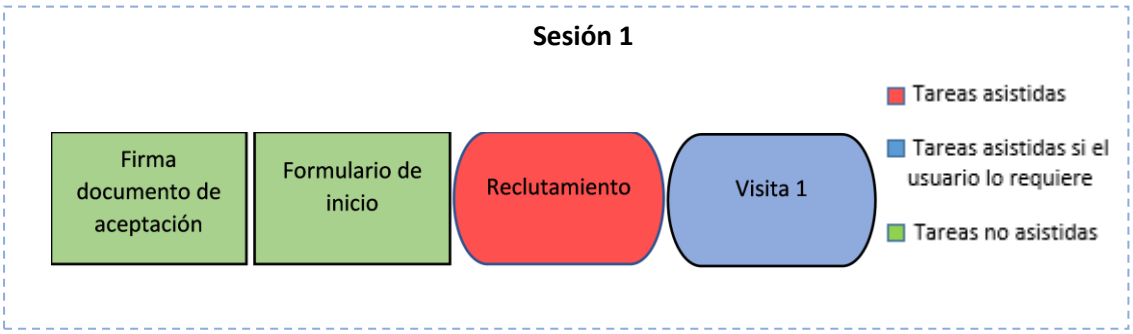

Figura 6. Esquema sesión 1

- **Sesión 2.** Cuando el usuario acude por segunda vez a la evaluación, se realiza las siguientes tareas (Figura 7):

    - **Verificación 2.** Tras haber transcurrido al menos una semana desde que se realizara la visita 1 al cajero, el usuario realiza una segunda visita donde debe retirar dinero del cajero haciendo uso de la aplicación. Se intenta que el usuario realice todas las tareas por sí mismo sin que el examinador tenga que intervenir. Una vez completada esta sesión, el usuario responderá un formulario final.

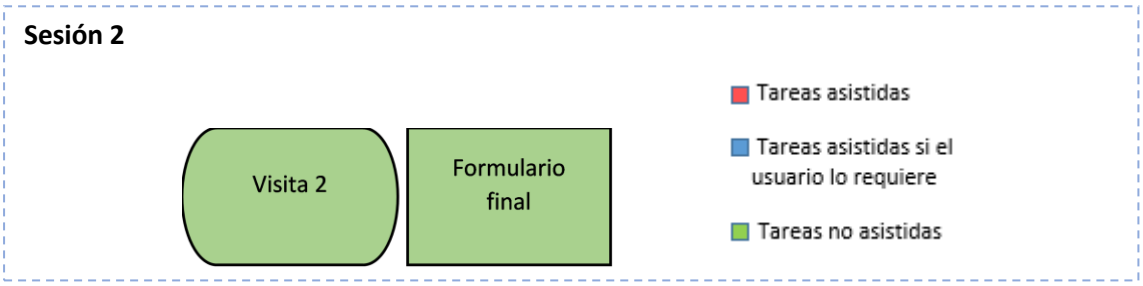

Figura 7. Esquema sesión 2

A continuación, se van a explicar más en detalle las fases que componen las dos sesiones de nuestra evaluación.

4.2. Reclutamiento y verificación 1

A continuación, se va a explicar en detalle en que consiste la sesión 1, mostrando un diagrama de flujo al final de cada punto, donde de forma gráfica se podrá tener una idea del proceso seguido en cada caso (Figura 15 y Figura 23).

4.2.1. Reclutamiento

El reclutamiento es la primera fase de nuestra evaluación. Durante esta etapa, el usuario sigue los pasos mostrados en la Figura 15 que aparece al final de este punto.

1. En primer lugar, la persona que se presenta a esta evaluación debe firmar un documento por ley de protección de datos. En el documento se recoge cual es proceso que va a seguir durante la evaluación, que usos se van a hacer de sus datos personales/biométricos, así como que derechos tiene el usuario en caso de que en un futuro quiera que los datos desaparezcan de nuestra base de datos. El documento de protección de datos se adjunta en el anexo 1 al final de la presente memoria.

2. Una vez firmado el documento de protección de datos, el usuario rellena un cuestionario inicial para ver qué relación tiene con las tecnologías y que conocimientos tiene sobre el uso de biometría. El cuestionario de inicio se encuentra en el anexo 2 al final de la presente memoria.

3. Cundo ya se ha rellenado el cuestionario de inicio, se procede a reclutar a dicho usuario, Figura 8. Entendemos reclutar como la creación una base de datos, donde se recogen los datos personales y biométricos de todas las personas que realizan la evaluación.

Figura 8. Menú reclutamiento inicio Bioaccess.

4. Lo primero que nos pide la aplicación es introducir el nombre, apellido, edad, sexo y discapacidad, Figura 9. Es en este momento cuando se comienza a crear un documento Excel de forma automática, donde se asocia al usuario con un número de identificación y se comienzan a recoger numerosos datos de tiempos y errores que el usuario cometa, con la finalidad de poder realizar un estudio detallado de la aplicación y poder sacar conclusiones con respecto a la accesibilidad y usabilidad.

Figura 9. Menú reclutamiento información personal Bioaccess.

5. Después, se solicita al usuario que se tome 5 fotos seguidas de la cara haciendo uso de la cámara frontal que el teléfono móvil tiene incorporada. Para realizar estas 5 fotos el usuario debe enfocarse solo la cara y presionar el botón de capturar, intentando tener, en la medida de lo posible, un fondo lo más despejado y blanco posible, y, además, se debe evitar estar a contraluz Figura 10.

Figura 10. Menú reclutamiento fotos Bioaccess.

6. Tras la toma de fotos, la aplicación pide al usuario que introduzca un PIN cualquiera de 4 dígitos. Una vez Introducido, la aplicación le pide de nuevo el PIN para verificar si el usuario ha introducido el PIN que tenía en mente o, en caso de no coincidir con el primer pin, se le pedirá uno nuevo, Figura 11.

Figura 11. Menú reclutamiento código pin Bioaccess.

7. Tras crear un PIN, el usuario grabará su voz en el dispositivo móvil. Para ello, se leerá una frase que aparece en pantalla mientras se mantiene apretado el botón central que tiene imagen de micrófono. La frase a leer será: "Mi voz es la clave que no tengo que recordar". Este proceso se repetirá tres veces seguidas, hablando de forma clara y sin acelerar el ritmo de voz, Figura 12. Se decide usar esta frase ya que se considera una frase que todo el mundo puede comprender y asimilar de forma sencilla.

Figura 12. Menú reclutamiento de voz Bioaccess.

8. Tras procesar la voz, el usuario tendrá que crear un patrón de seguridad. Este proceso se realiza de igual forma que la creación del PIN, Figura 13.

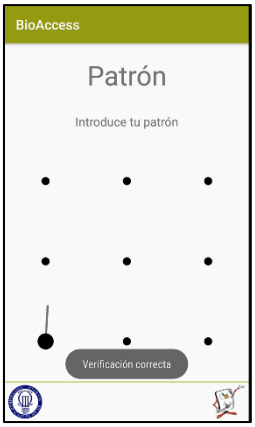

Figura 13. Menú reclutamiento patrón de seguridad Bioaccess

9. Por último, el usuario debe guardar la huella dactilar del dedo de la mano que él elija, pero tendrá que acordarse del dedo que ha usado para poder ser reconocido en ocasiones futuras. El reclutamiento de la huella es un proceso largo, ya que el usuario tendrá que situar y retirar la yema del dedo seleccionado del sensor varias veces, hasta que la aplicación móvil estime que es capaz de reconocer la huella del sujeto en cuestión. (El usuario tendrá que poner y retirar la yema del dedo del sensor una media de 15-20 veces hasta que se logra un mapa óptimo de la huella dactilar) Figura 14.

Figura 14. Menú reclutamiento huella dactilar Bioaccess.

A continuación, podemos ver un diagrama de flujo de todos los pasos que se acaban de explicar (Figura 15).

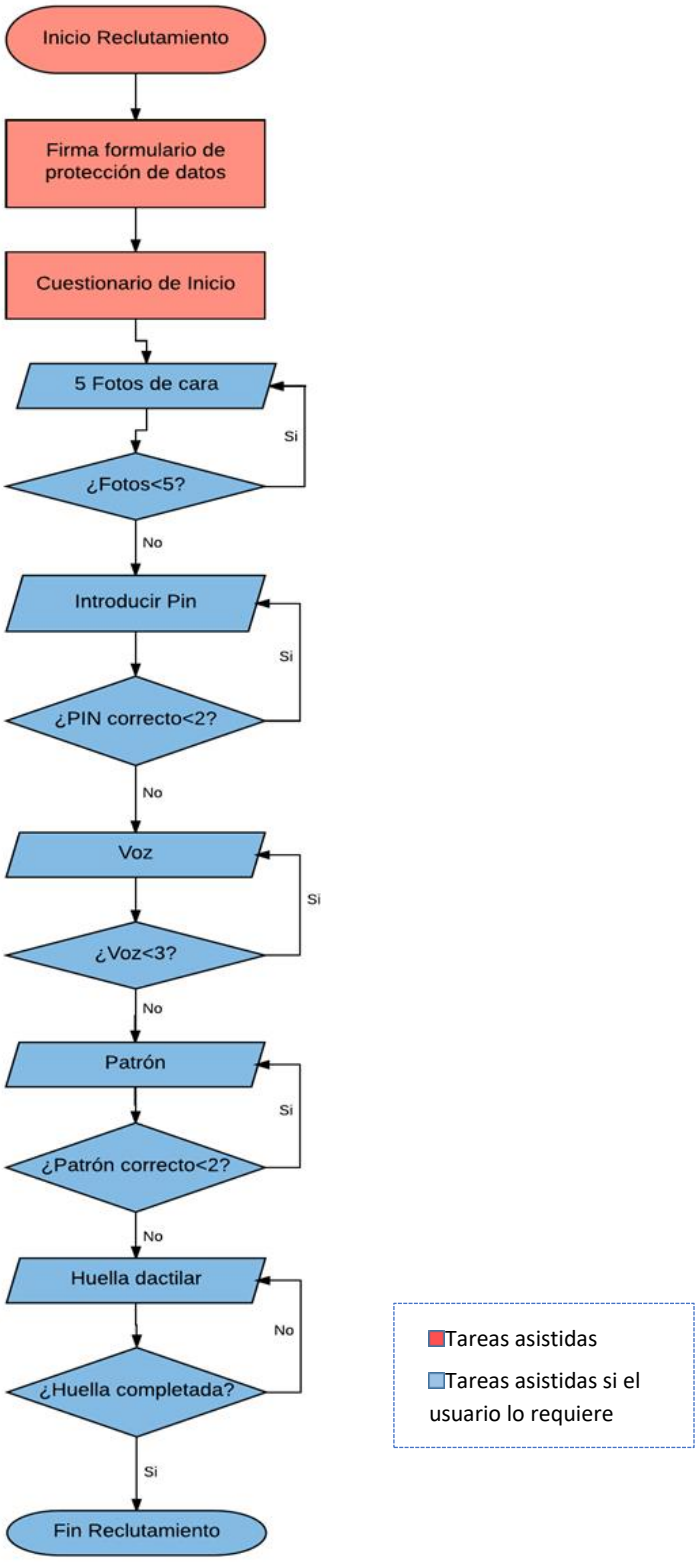

Figura 15. Diagrama de flujo del Reclutamiento

Durante el reclutamiento se asiste a los usuarios en todo lo que necesiten en cuanto al uso de la aplicación móvil se refiere. Es decir, se responde cualquier duda sobre cómo funciona o como se tiene que interactuar con la aplicación móvil, pero no se asistirá al usuario en las siguientes circunstancias:

- Si un usuario no puede realizar alguna de las tareas que se le propone durante el reclutamiento, nos podemos saltar dicha toma de datos, de tal forma que en las siguientes verificaciones no se tendrá en cuenta. Por ejemplo, si un usuario es incapaz de tomarse fotos del rostro por sí mismo, ya sea por dificultades físicas o, simplemente no quiere realizar este paso, nos lo podremos saltar y en las siguientes verificaciones la aplicación automáticamente no le pregunta por este tipo de reconocimiento, ya que no tiene almacenado dicho dato.

- El usuario posee tres oportunidades para realizar cada toma de datos. Si por cualquier circunstancia una toma de datos falla tres veces seguidas, se pasará a la siguiente modalidad y en las siguientes fases no se tendrá en cuenta. Por ejemplo, el usuario introduce un patrón de seguridad. Una vez introducido se solicita al usuario que lo confirme. Si al confirmar no coincide con el patrón introducido la primera vez, el usuario debe introducir un nuevo patrón y acto seguido confirmarlo. Si el usuario falla este paso tres veces seguidas, la aplicación salta a la siguiente toma de datos de tal forma que en las siguientes verificaciones no se solicitará el patrón de seguridad al no haber registrado ninguno en la base de datos.

4.2.2. Verificación 1

Nos encontramos ante la segunda fase de nuestra sesión 1. Esta recogida de datos tiene lugar el primer día de evaluación, después de haber realizado el reclutamiento.

Durante este proceso, se intenta simular que el usuario accede a un cajero automático a través del teléfono móvil, haciendo uso la aplicación "Bioaccess", la cual contiene los datos personales y biométricos del usuario que se han guardado con anterioridad durante el reclutamiento.

El dispositivo móvil se conecta con la Tablet, la cual imita a un cajero, a través de bluetooth. Los pasos que se siguen durante la visita1 aparecen en la Figura 23 situada al final de este punto:

1. El examinador, tras poner en situación al usuario explicándole el proceso que va a seguir durante esta visita, accede a la aplicación con la cuenta de la persona que vaya a realizar la prueba. Es el examinador quien selecciona la cuenta del usuario que va a realizar la visita (Figura 16), para evitar que se acceda con una cuenta incorrecta, ya que, si se accede con una cuenta de un usuario que ya ha realizado la visita 1 se borraran todos los datos de tiempos y fallos recogidos en el Excel.

Figura 16. Menú inicio verificación 1 Bioaccess

2. La aplicación pide al usuario que se identifique con su huella dactilar. El usuario tendrá que recordar que dedo ha usado durante la fase de reclutamiento y colocarlo sobre el sensor (Figura 17). La aplicación ofrece tres oportunidades seguidas para realizar este paso. En caso de no finalizar con éxito esta identificación se pasará al siguiente menú.

Figura 17. Menú huella dactilar verificación 1 Bioaccess.

3. Una vez reconocida o no la huella dactilar, se pide al usuario que se identifique realizando una foto de su rostro. El usuario se enfocará el rostro con la cámara frontal del móvil y pulsará el botón capturar (Figura 18).

Figura 18. Menú reconocimiento facial verificación 1 Bioaccess.

4. Tras tomar una foto del rostro, se pide al usuario que se identifique haciendo uso del código PIN que usó en el reclutamiento (Figura 19). Se vuelve a tener tres oportunidades para realizar esta identificación. En caso de agotar todas las oportunidades seguiremos con el siguiente menú.

Figura 19. Menú verificación código pin 1 Bioaccess.

5. Tras reconocer o no el PIN, el usuario debe identificarse usando su voz (Figura 20). Para ello leerá una frase que aparece en pantalla. La frase que se tiene que leer es la misma que en el reclutamiento, "Mi voz es la clave que no tengo que recordar". Tras leer la frase hay que dejar de presionar el botón. El usuario vuelve a tener tres oportunidades para completar esta identificación. En caso de que se agoten los tres intentos, se pasará al siguiente paso.

Figura 20. Menú verificación 1 voz Bioaccess.

6. Tras haber reconocido la voz, la aplicación pide al usuario que se identifique con el patrón de seguridad que ha creado en el reclutamiento (Figura 21). Se vuelve a ofrecer tres oportunidades al usuario para completar esta identificación. En caso de que se agoten los tres intentos, se pasará al siguiente paso.

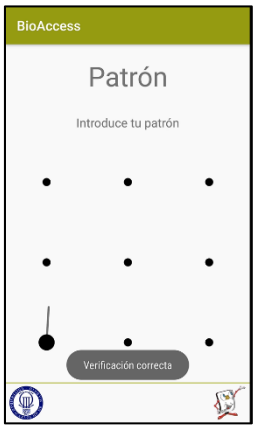

Figura 21. Menú verificación 1 Patrón de seguridad Bioaccess.

Una vez que se ha pasado por todas las etapas de seguridad, y aun que el usuario no haya superado alguno de los reconocimientos, la aplicación muestra en la pantalla del móvil un menú en el cual el usuario debe elegir entre sacar 20 o 50 euros del cajero (la tablet) Figura 22.

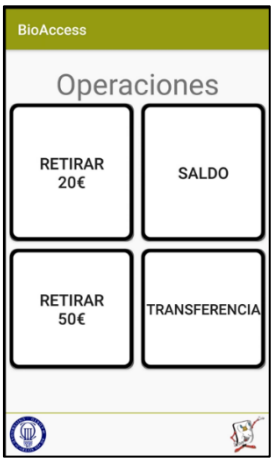

Figura 22. Menú de selección de la pantalla móvil para verificación 1.

Cuando el usuario selecciona una de estas dos opciones, la tableta muestra por pantalla una imagen que se corresponde al billete seleccionado desde la aplicación, mostrando a su vez un botón donde se puede seleccionar la opción de "Recoger".

Una vez que el usuario pulsa la opción "Recoger", la aplicación se sale de la cuenta del usuario de forma automática, y se podría volver a empezar el proceso

seleccionando un usuario. De esta forma, se intenta que en todo momento que la simulación sea lo más cercana a una situación real.

En la vida real, la aplicación se saldría de la cuenta bancaria o incluso podría bloquear dicha cuenta y mandar un mensaje al usuario siempre que no se complete algún paso de seguridad, pero, como queremos estudiar todo el proceso en su conjunto, necesitamos que el usuario pase por todos los menús a pesar de que no complete alguno de ellos.

A continuación, se muestra el diagrama de flujo del proceso que el usuario sigue al realizar la verificación 1 (Figura 23).

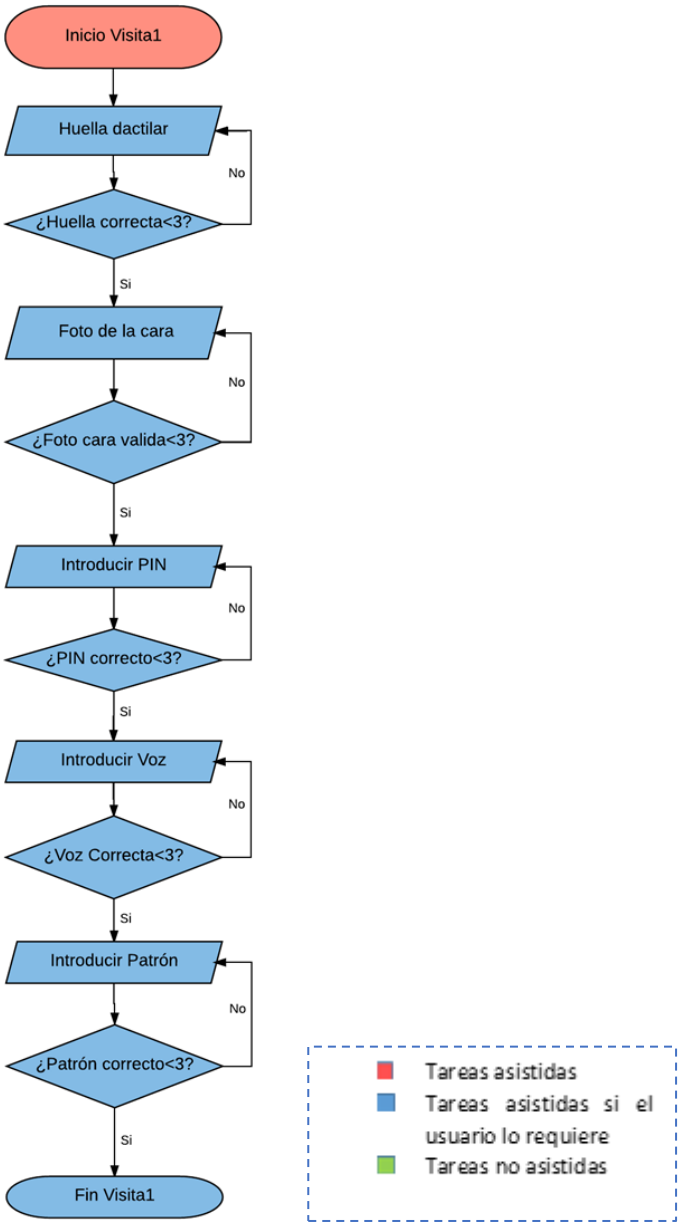

Figura 23. Diagrama de flujo verificación 1.

4.3. Verificación 2

Esta verificación, tiene lugar como mínimo una semana después de que el usuario haya realizado la verificación1. Durante este proceso se llevan a cabo los mismos pasos realizados durante la visita 1 con el objetivo de realizar un cuestionario final para recoger la opinión de cada uno y poder sacar conclusiones fiables sobre que biometría se considera más fácil, útil y segura.

Tan solo hay que tener en cuenta una gran diferencia con respecto a la visita1. En esta ocasión no se hará uso de la huella dactilar. La explicación de esta excepción es sencilla. Dado que al guardar y procesar la huella dactilar de cada usuario estamos usando la propia memoria y el propio código de programación del dispositivo móvil, tenemos un límite de huellas para guardar (en total en este móvil, la tecnología Android nos permite guardar 5 huellas. Al tratarse de código interno del móvil, está protegido y no podemos tocar en él). Por lo que tras realizar la visita1 y haber dejado pasar una semana, se ha atendido a muchos más usuarios, sobrescribiendo las huellas guardadas de anteriores visitas.

Los pasos a seguir durante la verificación 2 son los siguientes (las imágenes de todas las modalidades que tienen lugar durante la verificación 2 coinciden con las ya mostradas en la verificación 1, es por ello por lo que no se volverán a mostrar las figuras):

1. El examinador, tras poner en situación al usuario explicándole el proceso que va a seguir y que se pretende simular, accede a la aplicación con la cuenta de la persona que vaya a realizar la prueba para evitar que esta accede con una cuenta que no sea la suya (Figura 24).

Figura 24. Menú inicio verificación 2 Bioaccess.

2. La aplicación pide al usuario que se identifique tomándose una foto de su rostro.

3. Tras verificar el rostro, el usuario tiene que identificarse con su propio PIN que debe recordar.

4. Tras verificar el PIN, se pide al usuario que se identifique con su voz. Para ello, como en ocasiones anteriores, el usuario tiene que leer la frase que aparece por pantalla mientras se presiona el botón que aparece por pantalla que simula un micrófono. La frase será la misma que en ocasiones anteriores, "Mi voz es la clave que no tengo que recordar".

5. Una vez verificada la voz, el usuario tendrá que introducir su patrón, el cual debe recordar.

Durante toda esta visita 2, el usuario no recibirá ningún tipo de indicación ni ayuda, con la finalidad de obtener resultados objetivos que nos ayuden a medir la accesibilidad y utilidad de la aplicación móvil usada.

Al igual que en la visita 1, una vez que se ha pasado por todas las etapas de seguridad, la aplicación muestra en la pantalla del móvil un menú en el cual el usuario debe elegir entre sacar 20 o 50 euros del cajero automático.

Cuando el usuario selecciona una de estas dos opciones la tableta muestra por pantalla una imagen que se corresponde al billete seleccionado desde la aplicación, y muestra por pantalla un botón donde pone "Recoger".

Una vez que el usuario pulsa este botón, la aplicación se sale de la cuenta del usuario de forma automática, y se podría volver a empezar el proceso seleccionando un usuario.

Tras terminar todo el proceso, el usuario rellenará un cuestionario denominado "cuestionario final ". Dicho formulario se adjunta al final de esta memoria en el anexo 3 y en él se realizan una serie de preguntas para valorar cual es la biometría que más satisface al usuario en función de su experiencia, así como que sensación ha tenido con los dispositivos usados, intentando detectar si estos son incómodos.

Por otro lado, el examinador está tomando notas de todo lo que sucede a lo largo de toda la evaluación, es decir, se apuntan los fallos que da la aplicación, las dificultades que tiene el usuario a la hora de usar la aplicación, si existe algún proceso que el usuario no puede completar por sí mismo y no se llega a realizar pasando a la siguiente etapa. También se van apuntando opiniones que los usuarios van dando a lo largo de todo el proceso.

A continuación, se muestra el diagrama de flujo seguido durante la verificación 2 y que se acaba de explicar detalladamente (Figura 25).

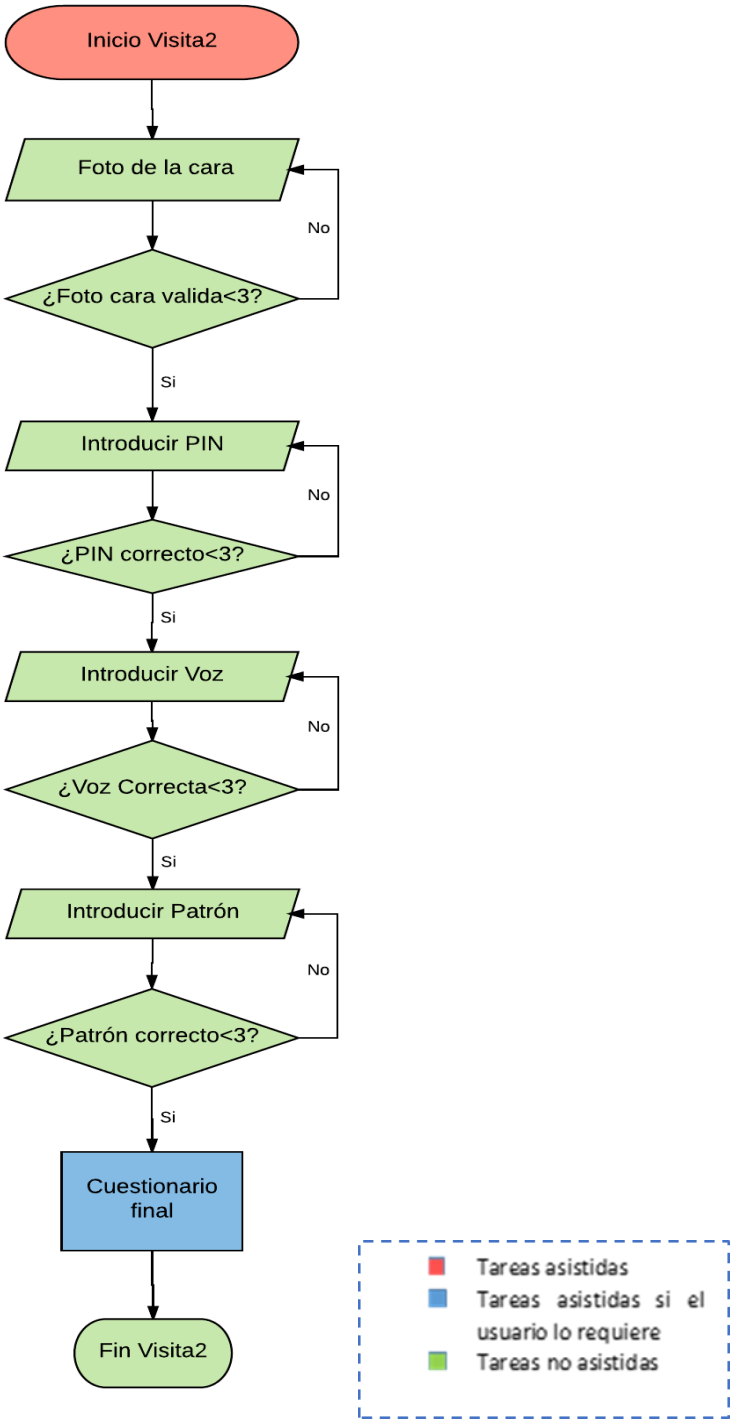

Figura 25.Diagrama de flujo verificación 2.

4.4. Software

Para realizar esta evaluación se ha hecho uso de numerosos algoritmos para llevar a cabo las diferentes medias biométricas, así como la toma del código pin y del patrón de seguridad. A continuación, vamos a nombrar y a dar una breve explicación de cada uno de ellos por separado.

4.4.1. Algoritmo de huella dactilar

Las huellas dactilares se recogen utilizando la interfaz de Android, la cual está disponible en los teléfonos inteligentes que llevan incorporado el sensor de huellas dactilares. Esta interfaz tiene un límite establecido de 5 huellas digitales que se pueden almacenar en un solo dispositivo móvil, por lo que, en este aspecto, el experimento está restringido, ya que no es posible utilizar la huella digital durante la visita 2.

El sistema de reconocimiento de huella digital no permite extraer imágenes ni permite obtener resultados numéricos. Tan solo devuelve un sí si la lectura de huella es correcta y un no en caso contrario.

4.4.2. Algoritmo de voz

El sistema de reconocimiento de voz (herramienta Kivox 360 [19]) fue proporcionado por la empresa Agnitio, y devuelve información de rendimiento y la calidad de cada muestra en particular.

Sin embargo, no todos los resultados que proporciona la herramienta se explican en esta memoria ya que carecen de utilidad en esta evaluación. En definitiva, para este experimento, la muestra de voz se envía a un servidor que devuelve un parámetro de calidad y una decisión (sí/no) al ser comparada con un patrón. Hemos normalizado el parámetro de calidad a "suficiente" o "baja".

4.4.3. Algoritmo de detección facial

No se aplicó ningún algoritmo en cuanto a reconocimiento facial durante la captura de muestras. Los usuarios simplemente se tomaron autofotos de su rostro siguiendo las indicaciones del examinador.

Una vez finalizada la toma de datos, se aplicó un algoritmo de detección de cara usando MATLAB [20]. El número de caras detectadas es utilizado como un parámetro de calidad de la muestra, de tal forma que se comprueba si los usuarios son capaces de

tomar correctamente autofotos del rostro adecuadas para un correcto reconocimiento facial.

Posteriormente, las imágenes son recortadas y se introducen en un algoritmo basado en SIFT (Scale-Invariant Feature Transform) [21], con el fin de ser comparadas con las imágenes de referencia tomadas durante la etapa de reclutamiento.

SIFT es un algoritmo usado en visión artificial para extraer características relevantes de las imágenes que posteriormente pueden usarse en reconocimiento de objetos, detección de movimiento, registro de la imagen y otras tareas. SIFT es un algoritmo resistente a los cambios de oclusión, escala y orientación. En nuestro caso, representa una imagen de la cara creando muchos descriptores. Para comparar dos imágenes representadas en sus respectivos conjuntos de descriptores SIFT se calcula una distancia euclidiana entre ellos. Si su distancia es inferior a un umbral prefijado, los descriptores locales de ambas imágenes se consideran coincidentes. El resultado de coincidencias finales se calcula como el número de descriptores pareados divididos por el número de descriptores disponibles [21].

4.5. Hardware usado

Para realizar la evaluación, los usuarios interactúan con un dispositivo móvil inteligente, el cual tiene instalada la aplicación Bioaccess. Dicha aplicación está conectada vía Bluetooth con una Tablet que simula un cajero automático ficticio.

4.5.1. Dispositivo móvil

El dispositivo móvil seleccionado es un Smartphone 3T OnePlus (Figura 26, tamaño 152.7x74.7x7.35 mm y 5.5 pulgadas de pantalla). Se decide usar este dispositivo ya que lleva incorporado un sensor de huella digital, una cámara frontal de 16 MP y su tamaño es suficiente para poder interactuar con él aparentemente sin dificultad.

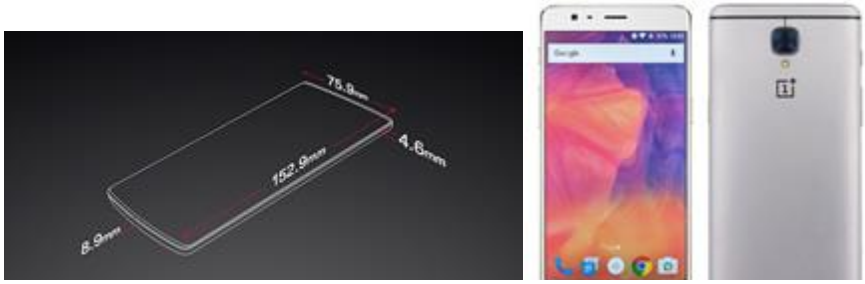

Figura 26. Dispositivo móvil 3T OnePlus

4.5.2. Tablet

El dispositivo usado es una Tablet Sony Xperia Z (Figura 27, tamaño 266x6.9x172 mm y 10.1 pulgadas de pantalla). Se decide usar este dispositivo debido a su amplia pantalla y a la posibilidad de poder conectarse con otros dispositivos vía bluetooth.

Figura 27. Tablet Sony Xperia Z

4.6. Escenario

La evaluación tuvo lugar en el Centro de Recuperación de Personas con Discapacidad Física de Madrid (CRMF) [1]. El CRMF es un Centro público al servicio de las personas con discapacidad física y/o sensorial de todo el Estado Español, que ofrece a sus usuarios un programa individual recuperador para facilitar su integración social y laboral, tomando en consideración sus aspiraciones e intereses.

En todo momento se tuvo en cuenta la norma de evaluación de escenario ISO/IEC 19795-2:2007" Testing *methodologies for technology and scenario evaluation*" [17]

El centro facilitó una sala grande, cómoda, iluminada y con paredes blancas para poder realizar sin problemas las sesiones con los usuarios.

Los dispositivos usados se sitúan sobre una mesa de acuerdo a las preferencias del usuario, siempre que pueda interactuar con ellos sin dificultad.

La evaluación de los usuarios que no pertenecen al CRMF se realizó en una habitación que cumplía las mismas condiciones mencionadas anteriormente, de tal forma que todos los usuarios se encontraran en ámbitos similares a la hora de realizar las pruebas.

4.7. Documentos

Para obtener resultados sobre nuestra evaluación, ha sido necesario que los usuarios cumplimentaran los siguientes documentos: documento de conformidad, documento, cuestionario de inicio y cuestionario final. Los dos últimos cuestionarios fueron creados haciendo uso de la aplicación "google forms", la cual nos permite sacar resultados de forma automática en Excel tras responder las preguntas.

4.7.1. Documento de conformidad

El objetivo de este documento es informar al usuario sobre el proceso en el que va a participar, así como del uso que se va a dar de sus datos personales. El documento se divide en las siguientes secciones:

- **Introducción.**

Se informa al usuario sobre el objetivo que se quiere conseguir con este proyecto. Se le informa también de la necesidad de recoger datos personales y biométrico destacando que el proceso no entraña ningún riesgo ni causa daños físicos a la persona.

- **Detalles del proceso.**

En este punto se indica al usuario que la evaluación se realiza a lo largo de dos sesiones en días distintos, dejando transcurrir como mínimo una semana entre cada sesión. Se informa al usuario de que siempre estará acompañado por una persona que le supervisará y le ayudará a lo largo del proceso, explicando cómo debe interactuar con los dispositivos.

- **¿Qué pasará con mis datos personales? ¿Cuáles son mis derechos ante la LOPD?**

En este apartado se puntualiza donde se han guardado los datos personales recogidos de cada usuario y con qué propósito. Se explica al usuario su derecho a exigir la eliminación de sus datos de la base de datos donde se encuentran guardados, proporcionando un correo electrónico de contacto donde pueden ejercer este derecho. Si el usuario no ejerce este derecho, al cabo de un año los datos son anonimizados para su estudio en posteriores investigaciones. Por último, se explica la confidencialidad de los datos personales que han sido guardados según la Ley Orgánica de Protección de Datos (LOPD).

Para que un usuario pueda participar en esta evaluación era obligatorio que se firmara este documento, dando consentimiento para el uso y procesado de sus datos personales. Dicho documento se puede se puede encontrar adjunto en la presente memoria en el anexo 1.

4.7.2. Cuestionario de inicio

La finalidad de este documento es conocer la opinión y experiencia que el usuario tiene sobre la biometría, así como la experiencia que el usuario tiene con la tecnología en general.

Este formulario puede encontrarse adjunto en el anexo 2.

4.7.3. Cuestionario final

La finalidad de este documento es conocer la opinión del usuario sobre los dispositivos a evaluar tras haber interactuado con ellos a lo largo de toda la evaluación. Para ello se realiza un conjunto de cuestiones con el objetivo de obtener el grado de satisfacción final.

Este formulario se puede encontrar adjunto en el anexo 3.

Capítulo 5

Pruebas y resultados

En este capítulo se van a analizar los datos obtenidos a lo largo de la evaluación, dividiendo los resultados en distintos grupos: características de los participantes, resultados de rendimiento, resultados de usabilidad, resultados de accesibilidad.

Dentro de cada grupo de resultados mencionado anteriormente, se va a diferenciar entre los resultados obtenidos con usuarios pertenecientes al CRMF y usuarios no pertenecientes al CRMF.

5.1. Características de los usuarios

Tal y como se ha comentado en puntos anteriores, la evaluación va dirigida a todas aquellas personas que tienen problemas de accesibilidad. Por ello, se ha realizado un estudio con personas pertenecientes al CRMF, que, de forma voluntaria, han accedido a participar en este proyecto.

Por otro lado, en esta evaluación también han participado personas ajenas al CRMF con la finalidad de ampliar el número de muestras y poder comparar sus resultados con los del grupo de personas del CRMF.

En definitiva, en la evaluación participaron un total de 41 usuarios, de los cuales 21 de ellos pertenecen al CRMF y los 20 restantes no presentaban ningún problema de accesibilidad.

A continuación, vamos a analizar las características de ambos grupos de usuarios.

5.1.1. Características usuarios CRMF

Como se ha comentado anteriormente, un total de 21 usuarios pertenecen a este grupo de personas con problemas de accesibilidad que, de forma totalmente voluntaria, han decidido formar parte de la evaluación.

Según el problema de accesibilidad que presenta cada usuario, podemos crear los siguientes subgrupos. Hay que tener en cuenta que un usuario puede pertenecer a más de un subgrupo:

- **Discapacidad de las manos y brazos.** El participante presenta imposibilidad o dificultad para usar las manos y los brazos adecuadamente a la hora de realizar tareas comunes. Esta circunstancia plantea dificultades para interactuar con el dispositivo móvil. Un total de 5 usuarios pertenecen a este subgrupo.

- **Discapacidad de las piernas.** Imposibilidad o dificultad para caminar correctamente. Debido a los elementos de ayuda que este grupo de personas utiliza (por ejemplo, silla de ruedas o muletas), pueden producirse inconvenientes a la hora de interactuar con los dispositivos como, por ejemplo, dificultades para manejar el dispositivo móvil con ambas manos.

- **Discapacidad visual.** Usuario con dificultad en percibir información visual.

- **Discapacidad cognitiva o dificultades de aprendizaje.** Imposibilidad o dificultad para entender instrucciones, memorizar pasos o hablar correctamente.

5.1.1.1. Género

Dentro del grupo de usuarios pertenecientes al CRMF podemos distinguir un total de 6 mujeres y 15 hombres (Figura 28).

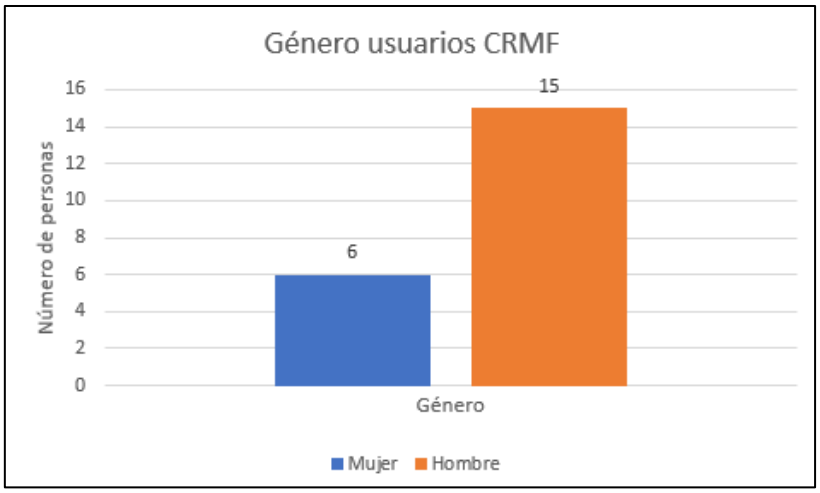

Figura 28.Género de usuarios pertenecientes al CRMF.

5.1.1.2. Intervalos de edad

Un total de 10 usuarios pertenecerán a un rango de edad de [18-30] años, 6 de ellos a un rango de [31-45] años, 3 de ellos a un rango de [46-60] años y 2 de ellos a un rango de [61-80] años (Figura 29).

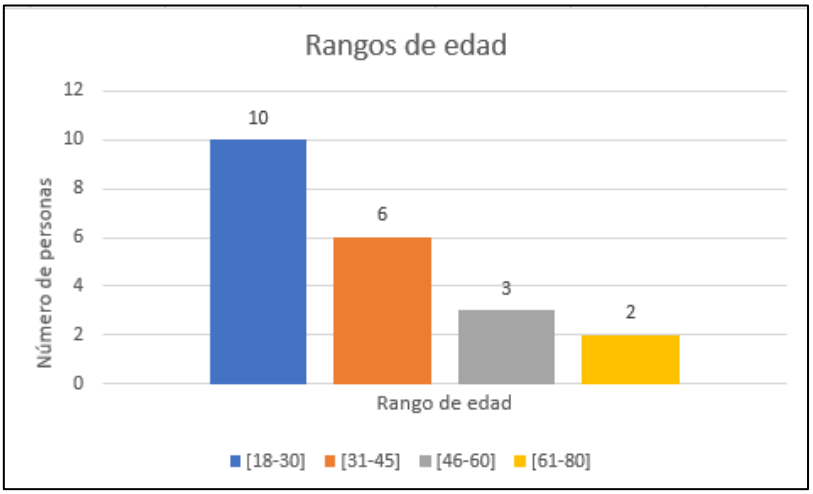

Figura 29.Rangos de edad usuarios CRMF.

5.1.1.3. Nivel de estudios

Tan solo 1 usuario no tenía ningún tipo de estudios, 9 de los usuarios tenía graduado escolar, 8 de ellos habían terminado bachillerato, y 3 usuarios tenían estudios universitarios (Figura 30).

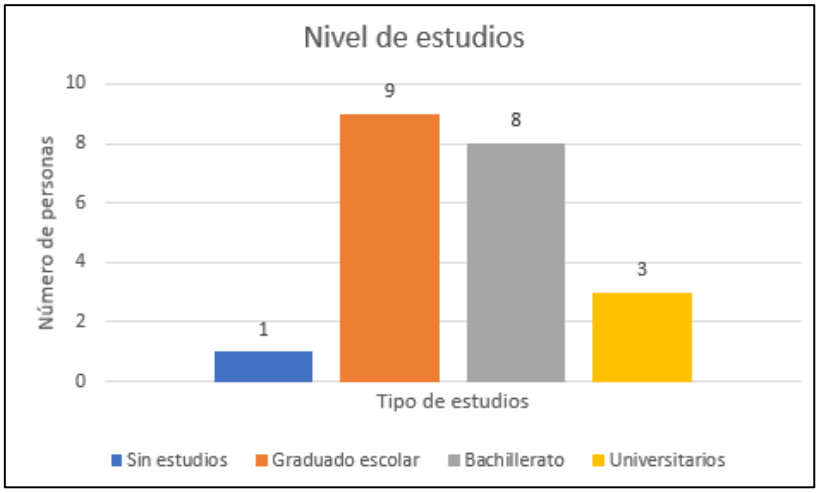

Figura 30. Nivel de estudios usuarios CRMF.

5.1.1.4. Lateralidad

Con respecto a la mano que los usuarios usan de forma habitual, tendremos 2 personas zurdas y 19 personas diestras (Figura 31).

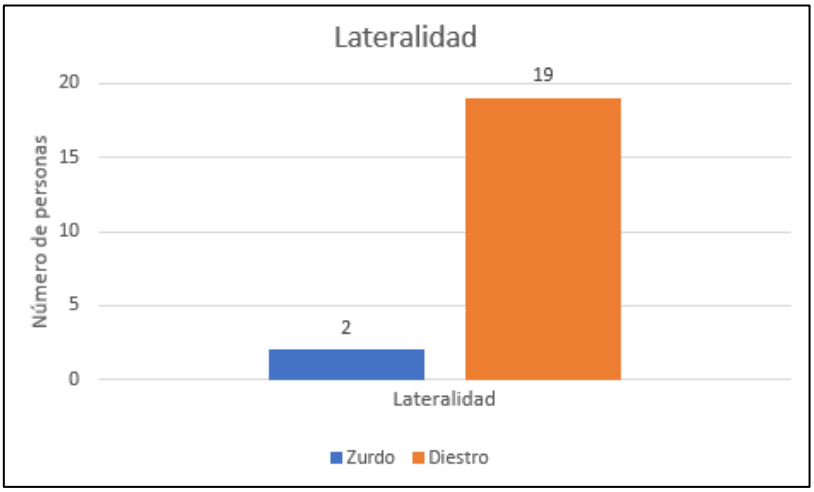

Figura 31. Lateralidad usuarios CRMF

5.1.2. Características usuarios no CRMF

Como se ha comentado anteriormente, tenemos 20 usuarios que pertenecen a este grupo de personas que no poseen ningún tipo de discapacidad o problemas de accesibilidad.

5.1.2.1. Género

Podemos distinguir un total de 16 mujeres y 4 hombres (Figura 32).

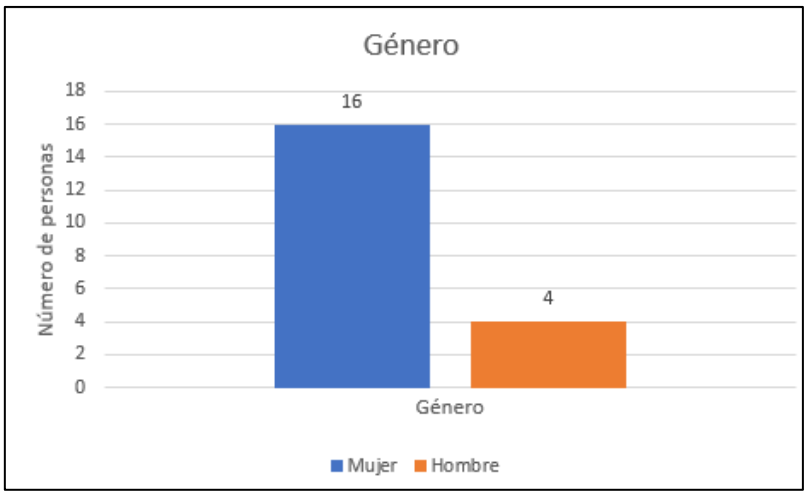

Figura 32. Género de usuarios no CRMF

5.1.2.2. Intervalos de edad

Un total de 15 usuarios pertenecerán a un rango de edad de [18-30] años, 2 de ellos a un rango de [31-45] años y 3 de ellos a un rango de [46-60] años. Ningún usuario superó los 60 años de edad (Figura 33).

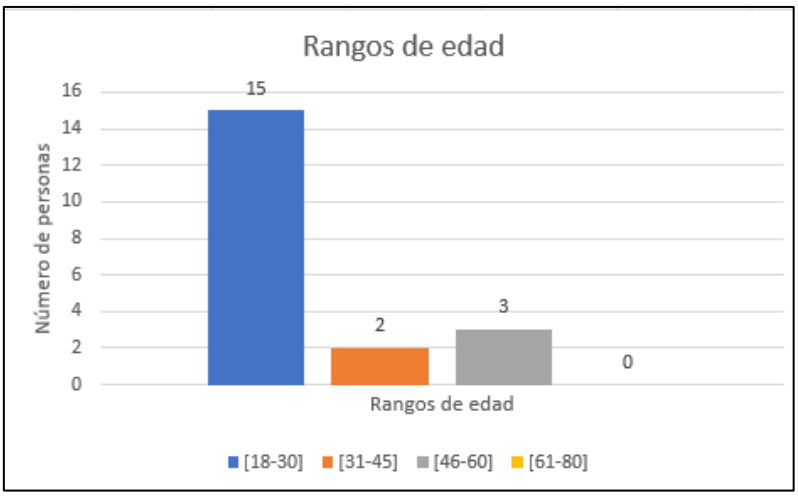

Figura 33. Rangos de edad usuarios no CRMF.

5.1.2.3. Nivel de estudios

Todos los participantes cuentan con algún tipo de estudio. Un total de 18 usuarios tienen estudios universitarios, 1 de ellos bachillerato y 1 usuario poseía graduado escolar (Figura 34).

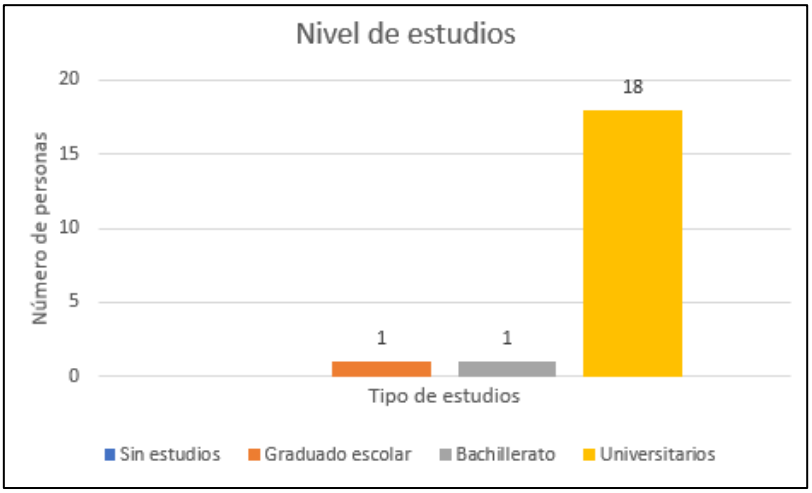

Figura 34. Nivel de estudios usuarios no CRMF.

5.1.2.4. Lateralidad

Con respecto a la mano que los usuarios usan de forma habitual en su vida cotidiana, tendremos 1 persona zurda y 19 personas diestras (Figura 35).

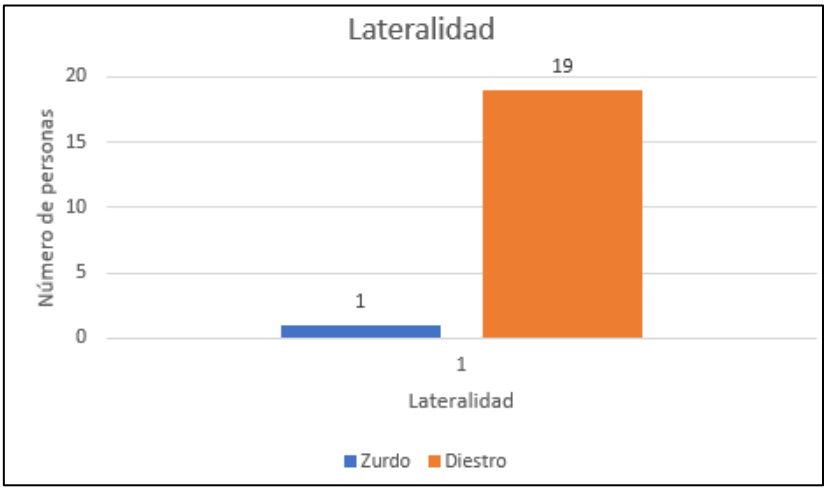

Figura 35. Lateralidad usuarios no CRMF.

5.2. Resultados del rendimiento

Este apartado contiene los resultados de las comparaciones de verificación tanto para las modalidades biométricas como no biométricas.

Las modalidades no biométricas como son el código pin y el patrón de seguridad, comparan la muestra que reciben con una plantilla y devuelven un "si" si los números son los mismo y un "no" en caso contrario.

En el reconocimiento de voz, la herramienta devuelve la calidad de los resultados, así como la comparación apareada (de un mismo usuario) entre la muestra recogida y la plantilla. La huella digital está gestionada por la tecnología Android del dispositivo móvil, y devolverá una decisión de "si" o "no" al comparar la muestra recogida con la plantilla. En el reconocimiento facial, para calcular los errores de verificación, se estableció un umbral y todos los resultados bajo el límite eran considerados como errores. Este límite se calculó a través de la comparación n:n de todas las imágenes recogidas en la base de datos, basándose la distancia de las muestras que pertenecen a la misma clase (FRR – Índice de falsos positivos) y entre clases (FAR-índice de falsos negativos). Sin embargo, como las comparaciones apareadas no son el objetivo de este trabajo, simplemente se contabilizan los errores de comprobaciones acopladas entre la plantilla y la muestra de un mismo usuario.

En definitiva, calculamos una comparación por verificación en cada modalidad, menos para el reconocimiento facial, donde tenemos acceso a las imágenes. En este último caso, se calculan 5 comparaciones por verificación (una por cada foto que el usuario se toma durante el reclutamiento), lo que da un total de diez comparaciones por usuario.

A continuación, vamos a analizar los resultados de rendimiento que aporta cada modalidad por separado, distinguiendo entre usuarios pertenecientes al CRMF y usuarios no CRMF. Además, dentro de usuarios CRMF crearemos subgrupos dependiendo de sus problemas de accesibilidad. Estos subgrupos serán:

- **Discapacidad de manos y brazos.** Lo denominaremos "DMB".
- **Discapacidad de piernas.** Lo denominaremos "DP".
- **Discapacidad visual.** Lo denominaremos "DV".
- **Discapacidad cognitiva o dificultades de aprendizaje.** Lo denominaremos "DCDA".

A partir de este momento y a lo largo del análisis de los resultados haremos uso de las siglas mencionadas a cada tipo de discapacidad para poder mostrar de forma más clara los resultados de rendimiento para cada modalidad.

A. Rendimiento del reconocimiento de voz

Tal y como se ha mencionado, el rendimiento de voz proporciona resultados de calidad y rendimiento.

En la Tabla 1 se expone el número de muestras de baja calidad obtenidas durante las distintas sesiones de la evaluación para cada grupo de usuario. Este número de muestras de baja calidad aparecen divididas por el número de muestras proporcionadas. El número de muestras por grupo depende del número de usuarios de cada grupo.

Usuarios		Sesión		
		Reclutamiento	Visita 1	Visita 2
CRMF	DMB	0/1	2/5	0/5
	DP	0/33	2/11	2/11
	DV	0/6	0/2	0/2
	DCDA	0/17	6/17	1/17
No CRMF		0/60	0/60	0/60

Tabla 1. Número de errores de voz adquiridos de las muestras de baja calidad divididos por el número total de muestras por grupo.

En la Tabla 2 se muestra los errores de verificación en cada visita divididos por el número total de muestras por grupo, el cual depende del número de usuarios de cada grupo y de las muestras rechazadas por baja calidad.

Un error de verificación se produce cuando la semejanza entre la muestra y la plantilla es inferior al umbral prefijado. Como se ha explicado en puntos anteriores, cada usuario tenía que completar una verificación y para ello disponía de tres intentos.

Usuarios		Sesiones	
		Visita 1	Visita 2
CRMF	DMB	0/3	0/5
	DP	0/9	2/9
	DV	0/2	1/2
	DCDA	0/11	0/16
No CRMF		0/60	0/60

Tabla 2. Número de errores de verificación dividido por el número total de muestras por grupo.

B. Rendimiento del reconocimiento facial

En la Tabla 3 se muestra el número de caras no detectadas por los diferentes grupos durante las dos visitas divididas por el número de muestras por grupo. Este número de muestras por grupo depende del número de usuarios de cada grupo.

Usuarios		Sesión		
		Reclutamiento	Visita 1	Visita 2
CRMF	DMB	1/26	1/6	1/6
	DP	2/57	1/12	0/11
	DV	0/10	0/2	0/2
	DCDA	2/87	0/17	0/17
No CRMF		3/100	3/103	0/20

Tabla 3. Número de caras no detectadas durante la evaluación dividido por el número total de muestras por grupo.

En la Tabla 4 se muestra el número de errores de verificación de cara en cada sesión. Es importante destacar que en esta Tabla no se recogen los usuarios que no pudieron completar la verificación de la cara, así como las imágenes que no tenían calidad suficiente.

Usuarios		Sesión	
		Visita 1	Visita 2
CRMF	DMB	5/24	6/24
	DP	13/54	23/55
	DV	4/10	8/10
	DCDA	10/85	26/85
No CRMF		24/100	79/100

Tabla 4. Número de errores de verificación de cara durante la evaluación dividido por el número total de muestras por grupo.

C. Rendimiento reconocimiento de huella dactilar

Todos los usuarios que participaron en esta modalidad realizaron el reclutamiento de forma correcta.

En la Tabla 5 se recoge los errores de verificación del reconocimiento de huella dactilar durante la visita 1 divididos por el número total de muestras por grupo. Dicho número total de muestras por grupo depende del número de usuarios por cada grupo.

Usuarios		Sesión
		Visita 1
CRMF	DMB	0/5
	DP	1/11
	DV	0/2
	DCDA	0/17
No CRMF		0/20

Tabla 5. Número de errores de verificación de huellas dactilares durante la evaluación dividido por el número total de muestras por grupo.

D. Rendimiento del código pin

En esta etapa los errores aparecen cuando los usuarios olvidan el código pin que han creado incluso durante el reclutamiento, así como cuando los usuarios no son capaces de pulsar correctamente la pantalla del dispositivo móvil por discapacidad en las manos.

En la Tabla 6 se muestra el número de errores al introducir mal el código pin durante las distintas fases de la evaluación divididas por el número total de entradas de pin por grupo. El número total de entradas de pin por grupo depende del número de usuarios de cada grupo.

Usuarios		Sesión		
		Reclutamiento	Visita 1	Visita 2
CRMF	DMB	1/15	4/8	3/7
	DP	0/33	0/11	6/15
	DV	0/6	0/2	3/4
	DCDA	1/51	6/20	12/25
No CRMF		0/60	0/20	16/30

Tabla 6. Número de errores al introducir el código pin dividido por en número total de entradas de pin por grupo.

E. Rendimiento del patrón de seguridad

Los errores de esta modalidad, al igual que los errores por el uso de pin, aparecen cuando los usuarios olvidan el patrón que ellos mismos crean.

En la Tabla 7 se muestra el número de errores al introducir el patrón de seguridad durante la evaluación dividido por el número total de entradas de patrón por grupo.

Usuarios		Sesión		
		Reclutamiento	Visita 1	Visita 2
CRMF	DMB	3/17	0/5	1/5
	DP	6/37	0/11	12/23
	DV	0/6	0/2	6/6
	DCDA	10/57	0/17	8/25
No CRMF		5/63	3/23	13/33

Tabla 7. Número de errores de entrada de patrón de seguridad dividido por el número total de entradas de patrón de seguridad por grupo.

5.3. Resultados de usabilidad

Aunque este experimento no pretende ser una evaluación completa de la usabilidad, ya que ésta conllevaría a seguir procedimientos y metodología adicionales a las que se van a llevar a cabo en proyecto, nos hemos basado en la definición de usabilidad ISO 9241:1998 ya mencionada en el punto "*2.8.1. Usabilidad*" con la finalidad de obtener resultados.

En definitiva, las métricas usadas en este apartado son:

- **La efectividad.** Depende del número de interacciones erróneas.
- **La eficiencia.** Depende del tiempo que se tarda en realizar las distintas tareas.
- **La satisfacción**. Depende del cumplimiento de las expectativas del usuario.

A continuación, vamos a entrar más en detalle en estos tres puntos mostrando los resultados obtenidos en cada uno de ellos.

5.3.1. Efectividad

Analizar la efectividad al completo, conllevaría mucho trabajo a parte del realizado. Por esta razón, a la hora de analizar la efectividad, solo hemos contabilizado el número de interacciones incorrectas del usuario con las distintas modalidades.

Con lo que a efectividad se refiere, son muchas las formas en las que el usuario puede realizar una mala interacción. De hecho, los propios usuarios descubren nuevas formas de poder interaccionar de manera incorrecta durante la evaluación.

En los siguientes apartados, vamos a analizar los errores de interacción más destacados que se producen en cada modalidad:

A. Efectividad del reconocimiento de voz

Consideramos interacciones incorrectas durante el reconocimiento de voz cuando el usuario tiene problemas para leer el texto, nerviosismo al hablar, problemas para presionar el botón central a la hora de hablar, inconvenientes al manipular el dispositivo móvil.

En la Tabla 8 se resume el número de interacciones erróneas que se han producido durante el uso de reconocimiento de voz detalladas por grupos y sesiones.

Usuarios		Sesión		
		Reclutamiento	Visita 1	Visita 2
CRMF	DMB	1/16	2/7	0/5
	DP	0/33	2/7	4/15
	DV	0/6	0/2	3/5
	DCDA	0/51	6/23	1/18
No CRMF		0/60	1/21	3/23

Tabla 8. Número de interacciones erróneas durante el reconocimiento de voz dividido por el número total de reconocimientos de voz por grupo

B. Efectividad del reconocimiento facial

Durante el reconocimiento del rostro, las interacciones incorrectas se producen cuando los usuarios intentan centrar la cara en la cámara sosteniendo el teléfono móvil con una mano y pulsando el botón de capturar para realizar la foto.

En la Tabla 9 se muestra el número de interacciones erróneas producidas durante el reconocimiento facial detalladas por grupos y sesiones.

Usuarios		Sesión		
		Reclutamiento	Visita 1	Visita 2
CRMF	DMB	1/26	1/6	1/6
	DP	2/57	0/11	0/11
	DV	0/10	0/2	0/2
	DCDA	2/87	2/17	0/15
No CRMF		0/100	0/20	0/20

Tabla 9. Número de errores de interacción durante el reconocimiento facial dividido por el número de reconocimientos faciales por grupo.

C. Efectividad del reconocimiento de huella dactilar

Durante el reconocimiento de la huella dactilar, los errores de interacción se producen cuando el usuario no sitúa de forma el correcta el dedo sobre el sensor y/o no lo mantiene encima el tiempo adecuado.

En la Tabla 10 se muestra el número de interacciones erróneas producidas durante el reconocimiento de la huella dactilar.

Usuarios		Sesión	
		Reclutamiento	Visita 1
CRMF	DMB	0/15	0/5
	DP	0/33	0/11
	DV	0/6	0/2
	DCDA	1/52	0/17
No CRMF		2/62	1/21

Tabla 10. Número de errores de interacción durante el reconocimiento de huella dactilar dividido por el número total de reconocimientos dactilares por grupo.

D. Efectividad del pin y del patrón de seguridad

Los errores de interacción en las modalidades no biométricas tienen lugar cuando el usuario no puede interaccionar de forma adecuada con la pantalla táctil del dispositivo electrónico.

En las siguientes Tablas se muestra, por un lado, el número de usuarios que no pudieron usar pin o patrón durante las dos visitas, ya que durante el reclutamiento no completaron estas modalidades (Tabla 11) y, por otro lado, se muestra el número de usuarios que no pudieron completar el uso de pin o patrón en alguna de las visitas (Tabla 12).

Usuarios		Modalidad	
		PIN	Patrón de seguridad
CRMF	DMB	0	0
	DP	0	0
	DV	0	0
	DCDA	0	2
No CRMF		0	1

Tabla 11. Número de usuarios que no pudieron utilizar el código pin y el patrón de seguridad durante las visitas 1 y 2.

Usuarios		Modalidad	
		PIN	Patrón de seguridad
CRMF	DMB	1	2
	DP	2	6
	DV	1	2
	DCDA	4	4
No CRMF		5	4

Tabla 12. Número de usuarios completar el uso de pin o patrón durante alguna de las visitas.

5.3.2. Eficiencia

Dentro del estudio de la usabilidad también se debe analizar a eficiencia, en otras palabras, se debe analizar el tiempo que el usuario dedica a realizar cada una de las modalidades.

En este experimento, se ha medido el tiempo que el usuario emplea en cada modalidad y en cada sesión para comprobar el tiempo de evolución entre sesiones (lo que denominaríamos aprendizaje) y entre modalidades. Hay que destacar que el tiempo que los usuarios emplean en realizar el reclutamiento es mayor que el empleado en las visitas, ya que conlleva un mayor número de muestras en todas las modalidades.

A continuación, vamos a analizar cada modalidad por separado dividida por los diferentes grupos de usuarios según sus características.

A. Eficiencia del reconocimiento de voz

El tiempo que el usuario necesita para realizar el reconocimiento de voz comienza cando el usuario pulsa el botón para grabar su voz durante el primer intento y finaliza cuando se ha realizado la última grabación de voz (tendremos 3 muestras durante el reclutamiento y 1 durante las visitas).

En la siguiente Tabla se muestra la media y la desviación típica del tiempo empleado durante el reconocimiento de voz dividida en grupo de usuarios y sesiones (Tabla 13).

Usuarios		Sesión		
		Reclutamiento	Visita 1	Visita 2
CRMF	DMB	48,16 ± 9,23	16,05 ± 5,80	17,11 ±2,72
	DP	43,25 ± 11,46	10,77 ± 3,10	18,20 ± 6,90
	DV	33,35 ± 12,76	7,50 ± 0,80	17,28 ± 1,7
	DCDA	43,64 ± 9,70	13,70 ± 5,40	19,03 ± 10,52
No CRMF		34,24 ± 3,45	8,32 ± 2,03	11,31 ± 2,70

Tabla 13. Media y desviación típica del tiempo empleado por los usuarios durante el reconocimiento de voz mostrada por grupos y sesiones.

B. Eficiencia del reconocimiento facial

El tiempo que el usuario invierte durante el reconocimiento facial comienza cuando el usuario presiona el botón de capturar una primera vez y finaliza cuando el usuario se realiza la última foto (tendremos 5 tomas fotográficas durante el reclutamiento y 1 toma durante cada visita).

En la Tabla 14 se muestra la media y la desviación típica del tiempo empleado por los usuarios durante el reconocimiento del rostro detallado por tipos de usuario y sesiones.

Usuarios		Sesión		
		Reclutamiento	Visita 1	Visita 2
CRMF	DMB	24,30 ± 8,20	11,15 ± 3,71	10,05 ± 6,06
	DP	32,01 ± 8,70	9,70 ± 10,00	9,68 ± 4,06
	DV	31,71 ± 8,46	5,69 ± 1,78	8,36 ± 0,24
	DCDA	29,03 ± 7,09	8,72 ± 4,38	11,44 ± 6,29
No CRMF		28,14 ± 9,76	4,74 ± 1,83	6,49 ± 2,67

Tabla 14. Media y desviación típica del tiempo empleado por los usuarios durante el reconocimiento de voz detallado en grupos de usuario y sesiones.

C. Eficiencia del reconocimiento de huella dactilar

El tiempo que el usuario invierte durante el reconocimiento de huella dactilar se inicia cuando el usuario presiona el sensor por primera vez y termina cuando el usuario suelta el sensor por última vez (se necesitará una media de 20 muestras durante el reclutamiento y 1 para cada visita).

En la siguiente Tabla se muestra la media y la desviación típica que los usuarios emplean para realizar el reconocimiento de huella dactilar detallada por grupos de usuario y sesiones (Tabla 15).

Usuarios		Sesión	
		Reclutamiento	Visita 1
CRMF	DMB	72,58 ± 18,27	9,71 ± 5,18
	DP	59,38 ± 16,93	8,21 ± 4,58
	DV	52,61 ± 6,46	9,14 ± 0,91
	DCDA	72,15 ± 21,39	8,58 ± 4,45
No CRMF		64,39 ± 21,16	4,95 ± 2,53

Tabla 15. Media y desviación típica que los usuarios emplean para realizar el reconocimiento de huella dactilar mostrada por grupo y sesiones.

D. Eficiencia del código pin

El tiempo que el usuario necesita para realizar el reconocimiento del código pin comienza cuando se presiona el primer dígito y finaliza cuando se presiona el último dígito (esto ocurrirá tres veces durante el reclutamiento y 1 por cada visita).

En la Tabla 16 se muestra la media y la desviación típica del tiempo que los usuarios emplean para realizar el reconocimiento del código pin detallado por grupos de usuario y sesión.

Usuarios		Sesión		
		Reclutamiento	Visita 1	Visita 2
CRMF	DMB	25,42 ± 16,01	10,67 ± 4,02	11,25 ± 5,04
	DP	19,68 ± 12,57	8,15 ± 3,47	9,59 ± 6,45
	DV	15,61 ± 3,30	6,39 ± 0,67	7,23 ± 1,03
	DCDA	19,52 ± 11,30	8,03 ± 3,39	10,00 ± 5,56
No CRMF		10,46 ± 5,23	3,84 ± 1,01	5,19 ± 2,24

Tabla 16. Media y desviación típica del tiempo que los emplean para realizar el reconocimiento de código pin mostrado por grupos y sesiones.

E. Eficiencia del patrón de seguridad

El tiempo que el usuario necesita para realizar el reconocimiento del patrón de seguridad comienza cuando se presiona un punto de la malla de números que se ofrece por pantalla y finaliza cundo el usuario presiona el último punto (esto sucederá tres veces durante el reclutamiento y 1 vez por cada visita).

En la Tabla 17 se muestra la media y la desviación típica del tiempo que tardan los usuarios en realizar el reconocimiento del patrón de seguridad, detallando dicho tiempo en grupos de usuarios y sesiones.

Usuarios		Sesión		
		Reclutamiento	Visita 1	Visita 2
CRMF	DMB	14,28 ± 7,28	6,35 ± 2,59	7,58 ± 4,86
	DP	11,15 ± 6,24	4,66 ± 2,27	12,46 ± 9,01
	DV	10,48 ± 4,67	4,74 ± 1,09	-
	DCDA	13,04 ± 5,87	5,63 ± 2,36	8,25 ± 5,14
No CRMF		7,27 ± 514	3,10 ± 1,16	6,03 ± 4,41

Tabla 17. Media y deviación típica del tiempo que los usuarios emplean para realizar el reconocimiento por patrón de seguridad mostrado por grupos y sesiones.

5.3.3. Satisfacción

La satisfacción se obtiene a través de dos encuestas que los usuarios realizan antes de iniciar el reclutamiento y tras finalizar todas las sesiones que componen la evaluación. Además de las encuestas, el examinador va tomando notas de lo que considera importante a lo largo de las distintas sesiones. Las preguntas de las encuestas estaban relacionadas con la demografía (resultados que ya se han expuesto en el punto "5.1. Características de los usuarios"), preferencias sobre las modalidades y preferencias sobre reconocimiento biométrico.

A continuación, vamos a exponer los resultados a las preguntas realizadas en las encuestas antes y después de realizar el experimento.

1. ¿Qué preferiría utilizar? Huella/Reconocimiento facial/Voz/Pin/Patrón

a) Usuarios CRMF.

Antes de realizar la evaluación, los usuarios pertenecientes al CRMF dieron las siguientes respuestas (Figura 36): un 47.62% alegaron que preferían usar la huella dactilar como reconocimiento, seguido de un 19.05% de usuarios que preferían usar el código pin, un 14,29% preferían el uso del reconocimiento facial y un 9.52% preferían el uso del patrón y el reconocimiento de voz.

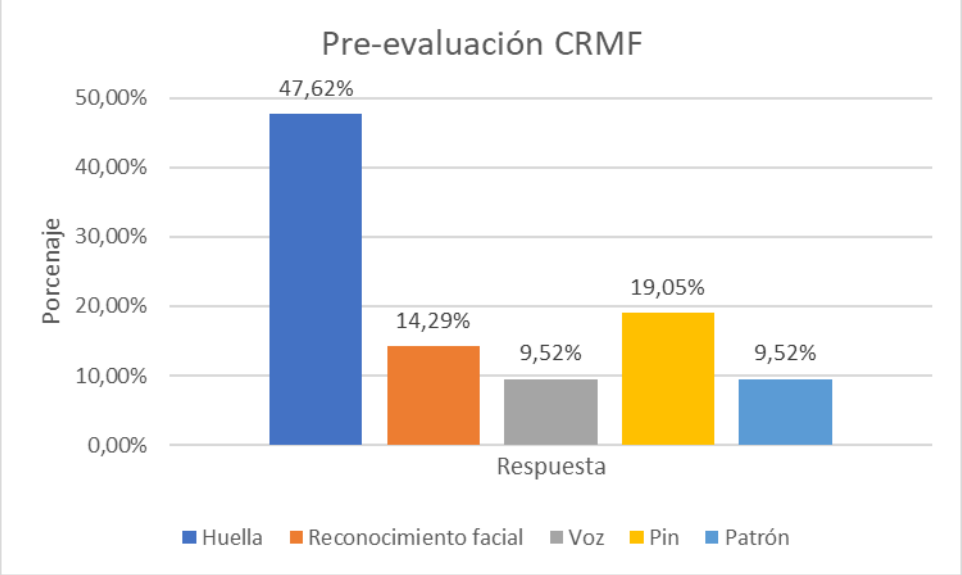

Figura 36. Resultados a la pregunta sobre preferencias de modalidad antes de realizar la evaluación de usuarios CRMF.

Tras realizar la evaluación las respuestas que los usuarios dieron a esta misma pregunta fueron las siguientes (Figura 37): un 43% de los usuarios prefieren el uso de la huella dactilar mientras que un 24% de os usuarios tienen preferencia por el reconocimiento facial, otro 24% se decanta por el uso del código pin, un 5% por el uso del reconocimiento de voz y finalmente un 5% de los usuarios prefiere el uso del patrón.

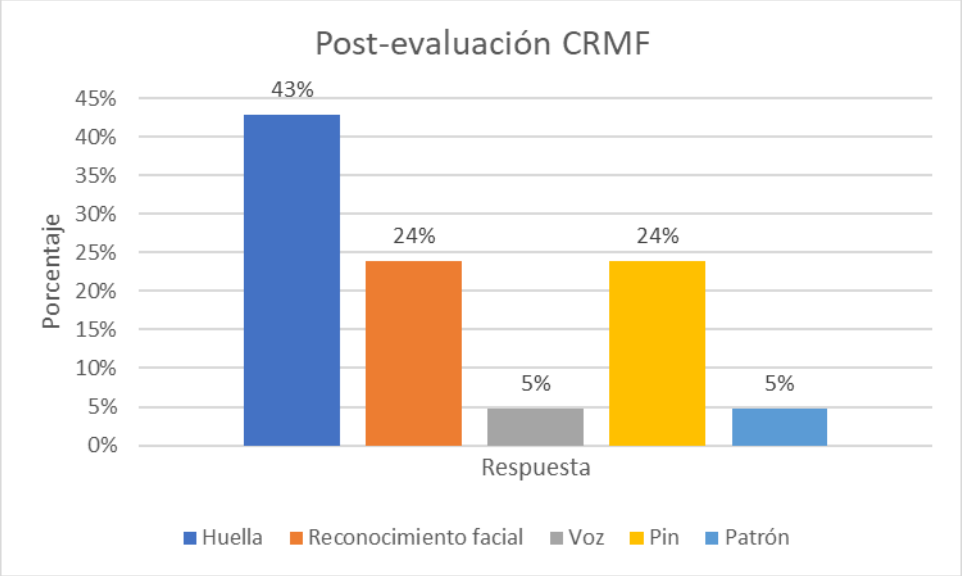

Figura 37. Resultados a la pregunta sobre preferencia de modalidad tras realizar la evaluación completa de usuarios CRMF

b) Usuarios no CRMF.

Antes de realizar la evaluación, los resultados sobre preferencia de modalidad para los usuarios no pertenecientes al CRMF fueron los siguientes (Figura 38): un 70% de los usuarios tienen preferencia por el uso de la huella dactilar, un 10% de ellos prefiere el uso de reconocimiento facial, un 10% el uso del patrón, un 5% el uso del reconocimiento de voz y finalmente, un 5% prefiere el uso del código pin.

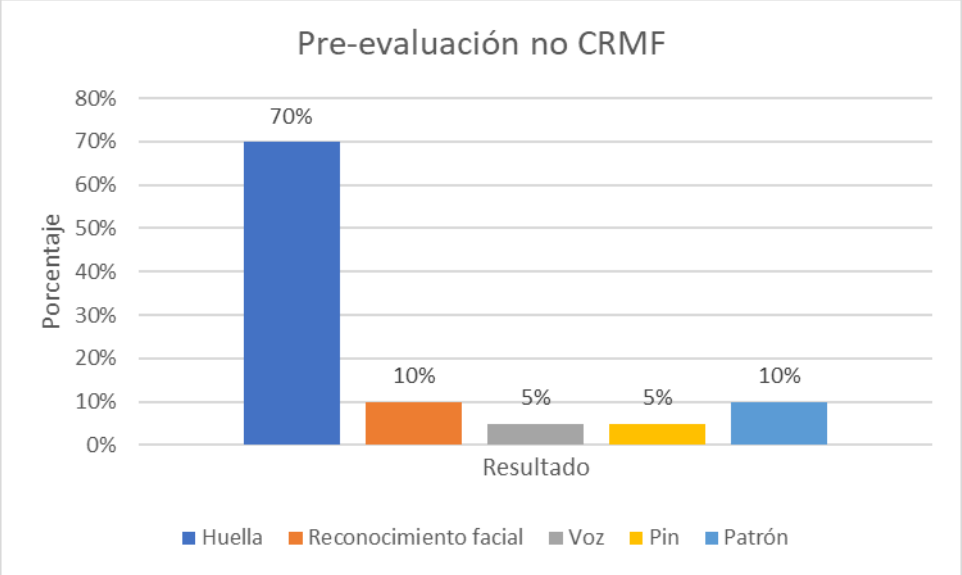

Figura 38. Resultados a la pregunta sobre preferencias de modalidad antes de realizar la evaluación de usuarios no CRMF

Tras realizar la evaluación las respuestas que los usuarios no pertenecientes al CRMF dieron a esta misma pregunta fueron las siguientes (Figura 39): un 65% de los usuarios preferían usar la huella dactilar, un 20% el uso del reconocimiento facial, un 10% el uso del reconocimiento de voz y un 5% el uso de código pin.

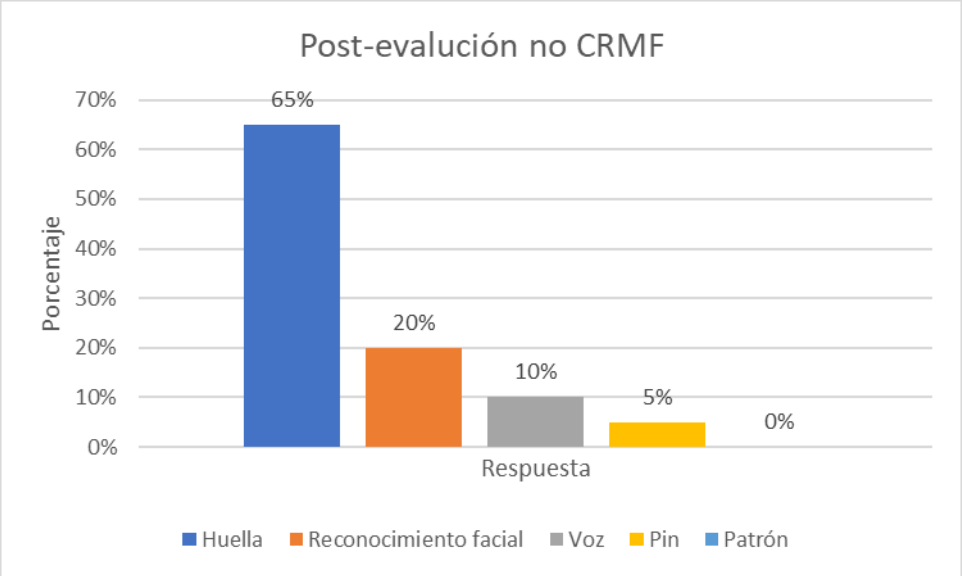

Figura 39. Resultados a la pregunta sobre preferencia de modalidad tras realizar la evaluación completa de usuarios no CRMF

2. **¿Utilizaría la biometría para realizar pagos, sacar dinero de un cajero, etc.? Si/No, porque no es lento/No, porque es incómodo/No, porque es inseguro/No, porque es difícil/Otro**

a) Usuarios CRMF

Antes de realizar la evaluación, los usuarios pertenecientes al CRMF respondieron a esta pregunta dando lugar a los siguientes resultados (Figura 40): un 57% de los usuarios del CRMF si usarían la biometría para realizar pagos o sacar dinero de un cajero mientras que un 43% no realizaría pagos o retiraría dinero de un cajero alegando seguridad.

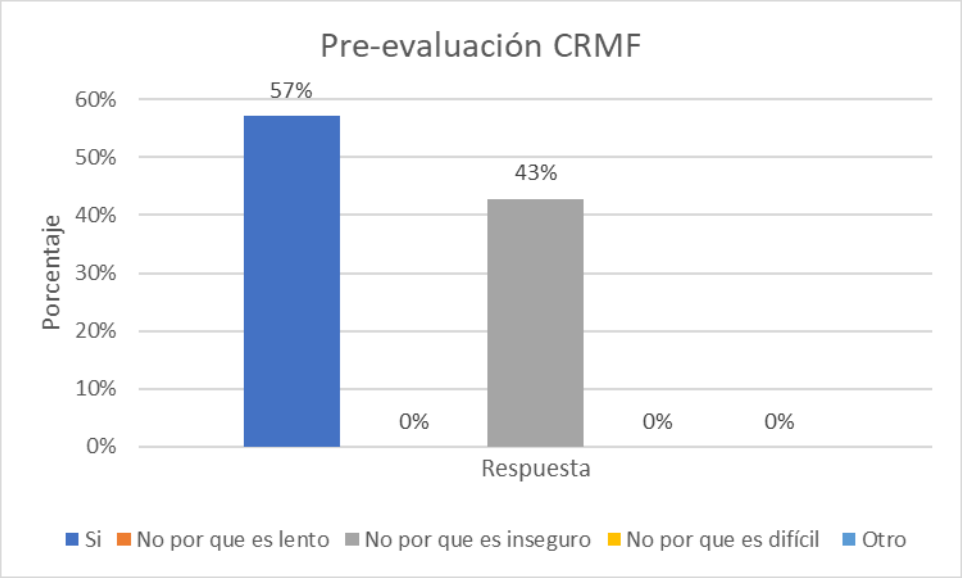

Figura 40. Resultados a la pregunta sobre uso de la biometría para realizar pagos o retirar dinero de un cajero antes de realizar la evaluación usuarios CRMF

Tras realizar la evaluación los usuarios respondieron la misma pregunta y los resultados fueron los siguientes (Figura 41): el 71% de los usuarios si realizarían pagos o retirarían dinero haciendo uso de la biometría mientras que un 29% no lo harían alegando razones de seguridad.

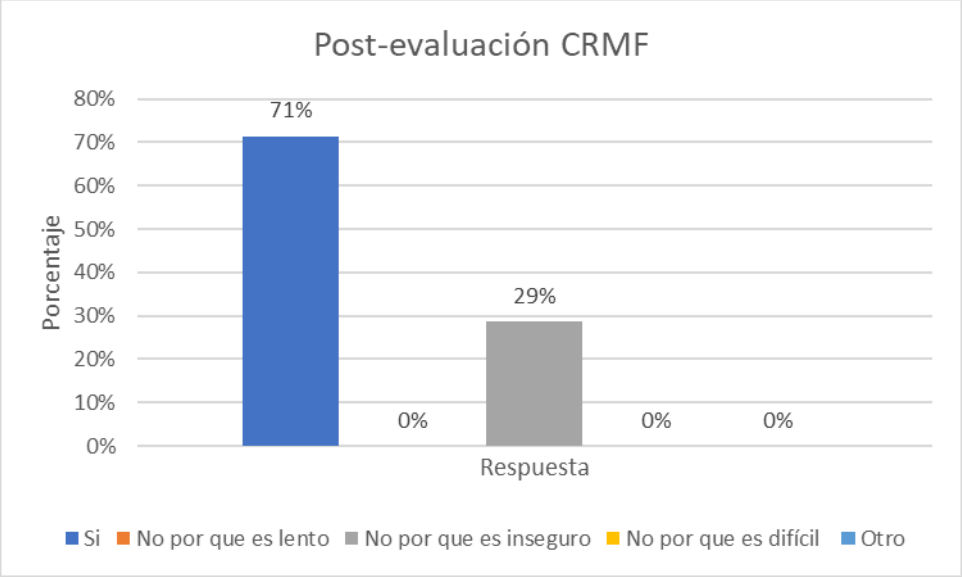

Figura 41. Resultados a la pregunta sobre uso de la biometría para realizar pagos o retirar dinero de un cajero tras realizar la evaluación usuarios CRMF

b) Usuarios no CRMF

Antes de realizar la evaluación, los usuarios no pertenecientes al CRMF tuvieron que responder la misma pregunta sobre si realizarían pagos o retirarían dinero de un cajero haciendo uso de la biometría y los resultados fueron los siguiente (Figura 42): 65% de estos usuarios aseguraban que si lo harían mientras que un 35% de ellos no lo harían alegando razones de seguridad.

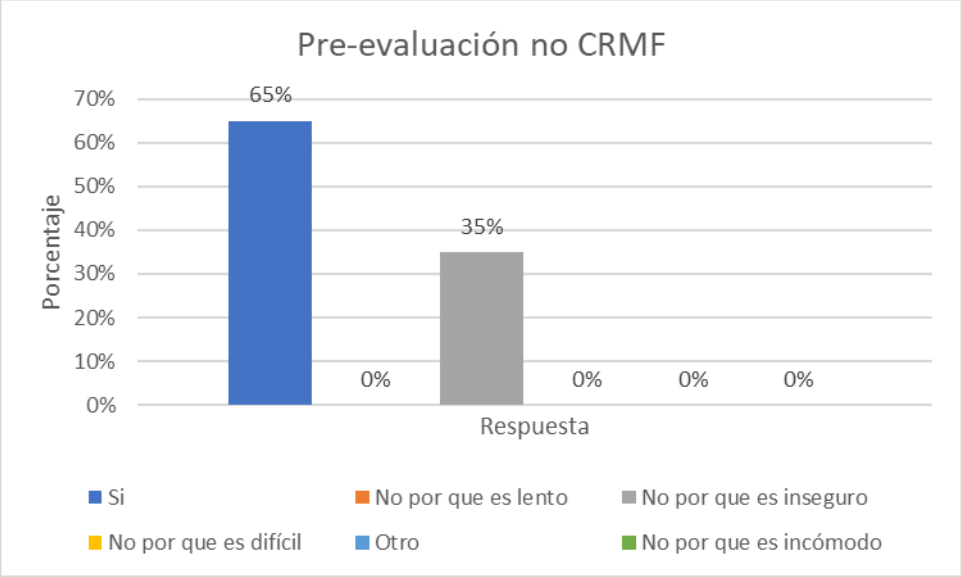

Figura 42. Resultados a la pregunta sobre uso de la biometría para realizar pagos o retirar dinero de un cajero antes de realizar la evaluación usuarios no CRMF.

Tras realizar la evaluación, los usuarios no pertenecientes al CRMF respondieron la misma pregunta y los resultados fueron (Figura 43): 85% de los usuarios si usarían la biometría para realizar pagos o sacar dinero mientras que un 15% de ellos continuaría sin usarla alegando razones de seguridad.

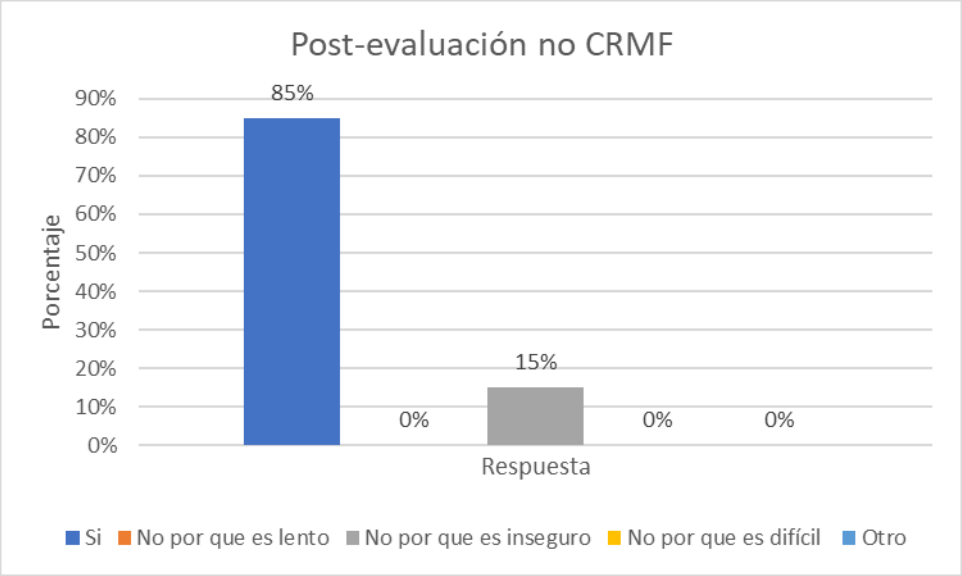

Figura 43. Resultados a la pregunta sobre uso de la biometría para realizar pagos o retirar dinero de un cajero tras realizar la evaluación usuarios no CRMF

5.4. Resultados de accesibilidad

En esta sección se muestra los resultados de la accesibilidad. Para conseguirlo, hemos medido dos factores que indican el gado en que los participantes podían completar el experimento y otro factor que está directamente relacionado con la aceptabilidad.

A continuación, se muestran dichos factores con sus respectivos resultados.

5.4.1. Número de usuarios que no pueden empezar una modalidad

Para los usuarios pertenecientes al CRMF, esta situación tiene lugar cuando el usuario no puede llevar a cabo las acciones requeridas debido a sus dificultades físicas o psíquicas.

Por otro lado, los usuarios que no pertenecen al CRMF son usuarios que no tienen problemas de accesibilidad a priori, pero pueden encontrar dificultades o incluso imposibilidad de utilizar alguna de las modalidades que se les plantea.

A continuación, se muestra el número de usuarios que no pueden iniciar las diferentes modalidades detallados en grupos (Tabla 18).

Usuarios		Modalidad				
		Voz	Cara	Huella dactilar	Pin	Patrón de seguridad
CRMF	DMB	0	2	0	0	0
	DP	0	0	0	0	0
	DV	0	0	0	0	0
	DCDA	1	2	0	0	2
No CRMF		0	0	0	0	1

Tabla 18. Número de usuarios que no pueden iniciar alguna modalidad.

5.4.2. Número de usuarios que no pueden completar una modalidad

Usuarios que comenzaron a usar una modalidad, pero no pueden completarla por problemas críticos, por ejemplo, el usuario olvidad el pin de seguridad o consume todos los intentos de reconocimiento de huella dactilar en alguna de las sesiones.

A continuación, se muestra los resultados de este tipo de errores detallados por grupos de usuario (Tabla 19).

Usuarios		Modalidad				
		Voz	Cara	Huella dactilar	Pin	Patrón de seguridad
CRMF	DMB	0	0	0	1	2
	DP	0	0	0	2	6
	DV	0	0	0	1	2
	DCDA	1	0	0	4	4
No CRMF		0	0	0	5	4

Tabla 19. Número de usuarios que no pudieron finalizar alguna modalidad.

5.4.3. Número de usuarios que no quieren iniciar una modalidad

Esta situación se produce cuando el usuario tiene desconfianza hacia la tecnología usada, temor a sufrir daños, nerviosismo u otras razones. Este último factor no puede ser considerado un parámetro de accesibilidad, pero si puede ser usado como un factor de aceptabilidad y confianza en la tecnología.

En la siguiente Tabla se muestran los resultados obtenidos detallados en grupo de usuario (Tabla 20).

Usuarios		Modalidad				
		Voz	Cara	Huella dactilar	Pin	Patrón de seguridad
CRMF	DMB	0	1	0	0	0
	DP	0	0	1	0	0
	DV	0	0	0	0	0
	DCDA	1	2	2	0	1
No CRMF		0	0	0	0	0

Tabla 20. Número de usuarios que no han querido iniciar alguna modalidad

Capítulo 6

Conclusiones y líneas futuras

En este capítulo, tras haber analizado todos los resultados se procederá a tomar conclusiones sobre la accesibilidad, el rendimiento y la usabilidad por separado. Además, se comentarán futuras mejoras, así como una guía de buenas prácticas de accesibilidad en sistemas de reconocimiento.

6.1. Introducción

El análisis de este experimento permite derivar varias conclusiones y mejoras para ser aplicadas en otros experimentos y diseños de sistemas biométricos.

Las conclusiones se van a obtener realizando un repaso de los resultados obtenidos y se van a dividir en tres grupos importantes: accesibilidad, usabilidad y rendimiento.

6.2. Rendimiento

Con respecto a la calidad de la muestra en el reconocimiento de voz y de cara, hay una gran diferencia entre los usuarios que no pertenecen al CRMF (apenas existen errores) y los usuarios del CRMF. Esta situación destaca sobre todo durante el reconocimiento de voz, donde los usuarios deben presionar un botón mientras hablan, lo que implica varias dificultades para los grupos DMB y DCDA. De hecho, la mayoría de los usuarios que pertenecen a estos grupos se quejó por la dificultad que entrañaba la tarea de presionar el botón mientras se leía la frase en voz alta.

Durante el reconocimiento facial, la mayoría de usuarios tenían dificultades para manejar el dispositivo móvil y enfocarse la cara, especialmente los usuarios del grupo DMB. Las muestras de baja calidad que se han obtenido durante el reconocimiento facial con usuarios no pertenecientes al CRMF, se deben a condiciones de mala iluminación de la sala.

Según los datos registrados en la Tabla 2, Tabla 4, Tabla 5, Tabla 6 y Tabla 7, podemos clasificar el rendimiento de las distintas modalidades, en el contexto de este experimento, de mejor a peor (Figura 44):

Figura 44. Clasificación de modalidades de mejor a peor rendimiento

Hay que destacar que el uso de la huella dactilar y del reconocimiento de voz dieron lugar a muy pocos errores de verificación. Por otro lado, el reconocimiento facial ofreció muy malos resultados provocados por la dificultad que implicaba tomarse fotos del rostro para algunos grupos de usuarios, así como las malas condiciones del entorno (por ejemplo, poca iluminación de la sala o fondo no uniforme).

También es llamativo la cantidad de errores que se producen cuando los usuarios deben introducir su código pin o su patrón durante la segunda visita. Esto sucede debido a que se dejó pasar mínimo una semana entre sesión1 y sesión2, lo que daba lugar a que muchos usuarios olvidaran sus credenciales.

6.3. Usabilidad

Tal y como se ha visto anteriormente, los resultados de usabilidad se dividen en efectividad, eficiencia y satisfacción. Aunque estos términos guardan relación entre ellos, se van a analizar por separado.

6.3.1. Efectividad

Este factor solo se analizó en modalidades biométricas, ya que la efectividad del uso de código pin y del patrón de seguridad está incluida en los resultados de rendimiento.

El reconocimiento de voz es la modalidad que más errores de interacción tiene. Gracias a las notas recogidas y los testimonios de los usuarios, la mayoría de los errores en esta modalidad se producen a causa del botón que se debe presionar a la hora de grabar el mensaje de voz. Estas malas interacciones no causaron muestras de baja calidad ya que el sistema no detecto dichas muestras y, por lo tanto, no fueron procesadas.

En el caso de reconocimiento facial, las malas interacciones ocasionaron muestras de baja calidad.

En cuanto al reconocimiento de huella dactilar, se apreció durante la evaluación que algunos usuarios, a la hora de posicionar el dedo sobre el sensor no lo hacían de forma correcta, por ejemplo, hubo muchos casos en los que se rotaba el dedo encima del sensor. Aun en estos casos que se producía rotaciones sobre el sensor, las huellas eran verificadas correctamente.

6.3.2. Eficiencia

La mayoría de las modalidades muestran una desviación típica con respecto al tiempo bastante elevada, lo que significa que no todos los usuarios tenían los mismos problemas a la hora de interaccionar con los sistemas biométricos (esto sucede incluso con usuarios que tienen las mismas características).

En cuanto a eficiencia se refiere, se observa una curva de aprendizaje: los usuarios aprenden a usar los sistemas durante el reclutamiento (se aprecian tiempos largos en todas las modalidades), han adquirido práctica durante la visita 1 (los tiempos por modalidad son notablemente más cortos), y finalmente se observa una pérdida de práctica durante la visita 2 (los tiempos por modalidad sufren una subida con respecto a la visita 1).

Con respecto al uso del código pin, los usuarios se quejaron del tiempo que se necesitaba para realizar el reclutamiento de la huella dactilar, ya que el sistema Android necesita en torno a 20 muestras de huella dactilar para crear una plantilla fiable.

El uso del código pin y del patrón de seguridad dio lugar a los tiempos más cortos durante el reclutamiento, pero el uso del patrón fue una novedad para muchos usuarios que nunca lo habían usado. Sin embargo, el reconocimiento facial y de huella dactilar dieron lugar a tiempos más cortos durante la visita 1 y 2, una vez que los usuarios se habituaron a ellos.

Hay que destacar que los usuarios del CRMF pertenecientes al grupo DMB invirtieron más tiempo en la mayoría de las modalidades debido a los problemas que tenían a la hora de manejar el teléfono móvil. El grupo DCDA presenta diferencias notables en los tiempos empleados en realizar la visita 1 y la visita 2 debido, en la mayoría de casos, a pérdidas de memoria.

6.3.3. Satisfacción

Los usuarios pertenecientes al CRMF mostraron su satisfacción por las modalidades que requieren menos interacciones, especialmente por la modalidad de reconocimiento facial que muchos usuarios consideraron una moda. Sin embargo, al final de la evaluación el 24% de usuarios pertenecientes al CRMF prefieren seguir usando métodos tradicionales como el código pin, método que consideran más seguro que la biometría. Los usuarios del CRMF pertenecientes al grupo DCDA mostraron un gran interés por el uso del reconocimiento biométrico ya que no necesitan memorizar códigos o patrones.

Por otro lado, un 65% de los usuarios no pertenecientes al CRMF preferían el uso de la huella dactilar al finalizar la evaluación, frente al 20% que prefieren el uso de reconocimiento facial, el 10% prefieren reconocimiento de voz y un 5% prefiere el uso del código pin. Este hecho refleja el creciente uso de reconocimiento de huella dactilar en los dispositivos móviles, el cual es considerado un método más sencillo que los métodos tradicionales.

Antes de realizar el experimento, un 57% de los usuarios del CRMF y un 35% de los usuarios no CRMF no usarían la biometría para sacar dinero de un cajero o para realizar algún tipo de pago alegando razones de seguridad. Estos datos reflejan falta de confianza en las nuevas tecnologías que son más o menos desconocidas para la mayoría de los participantes. Al final de la evaluación, la confianza en el uso de la biometría para realizar pagos o sacar dinero de un cajero aumentó, dando lugar a que solo un 29% de usuarios del CRMF y un 15% de usuarios no CRMF alegaran razones de seguridad o incomodidad para no usar biometría.

6.4. Accesibilidad

Los usuarios que no fueron capaces de comenzar alguna modalidad son aquellos que requieren un mayor cuidado y nos son capaces de realizar numerosas actividades cotidianas por sí mismos.

Tan solo un usuario no perteneciente al CRMF, cuya edad estaba comprendida entre 60-81 años, no llegaba a comprender como se usaba el patrón de seguridad siendo imposible reclutar dicha modalidad.

Muchos usuarios fueron incapaces de recordar sus credenciales a la hora de introducir el pin o el patrón de seguridad durante la segunda visita.

Algunos usuarios del CRMF decidieron no completar alguna modalidad alegando motivos de seguridad, confianza, o invasión de privacidad. Esto sucedió sobre todo en las modalidades de reconocimiento facial y huella dactilar.

6.5. Guía de buenas prácticas y líneas futuras

A lo largo de la evaluación van apareciendo inconvenientes con los que no se había contado, se descubren nuevos métodos de afrontar alguna sección, o simplemente los propios usuarios plantean situaciones que no habían ocurrido antes. Es por ello que, en este punto, se van a exponer lecciones y sugerencias que han ido apareciendo a lo largo de todo el proyecto, con la finalidad de tenerlas en cuenta en trabajos futuros:

- Cuanto menor sean las interacciones con el sistema, mejor, ya que esto implica una menor posibilidad de producir interacciones erróneas y, a su vez, reduce el tiempo que el usuario emplea para realizar la tarea. Sin embargo, esta reducción de interacciones puede afectar negativamente al rendimiento del sistema.

- Las personas con problemas de accesibilidad sienten muchas veces nerviosismo y ansiedad cuando usan tecnologías que les resultan novedosas. Es por ello que se debe prestar una atención especial a este tipo de usuarios, de tal forma que se sientan totalmente tranquilos a la hora de realizar la evaluación.

- El reconocimiento de voz se considera una modalidad no intrusiva, es decir, se realiza de forma automática, pero, a la hora de introducir un botón que se debe presionar a la hora de grabar la voz, se podrían producir rechazos. En definitiva, un aumento de automatización en el proceso de reconocimiento de voz, puede derivar en una mejor aceptación por parte del usuario.

- Otro aspecto a mejorar en el reconocimiento de voz es la oración que el usuario debe leer. Muchos usuarios tienen problemas a la hora de leer la frase directamente de la pantalla (por ejemplo, la letra puede ser demasiado pequeña, o les tiembla demasiado el pulso siendo imposible realizar una lectura correcta). Una solución a estas situaciones sería repetir una frase que el sistema previamente ha emitido por altavoz.

- La introducción de novedades, especialmente las que obligan al usuario a interactuar con el sistema, puede dar lugar a rechazos. Por ejemplo, en evaluación que se ha realizado, a muchos usuarios no les gustaba usar el patrón de seguridad.

- A la hora de recoger muestras de la huella dactilar, la aplicación móvil que se ha usado muestra por pantalla una imagen de una huella dactilar (Figura 45). Esta situación confundía a los usuarios, quienes situaban el dedo encima de la imagen en lugar de situarlo en el sensor que el móvil lleva incorporado, dando lugar a tiempos más largos durante el reclutamiento, que ya de por si eran largos según las opiniones de los participantes.

Figura 45. Imagen del sensor de huella Bioaccess.

- Las soluciones de autenticación deben adaptarse particularmente a cada usuario, ya que, incluso cuando se han analizado los resultados por grupos acordes a las características de los usuarios, se ha obtenido una elevada variabilidad en los resultados finales.

Presupuesto

1. Autor

Alvaro Ludeña Sanchez-Bayuela

2. Departamento

Tecnología electrónica

3. Descripción del proyecto

-Título: Evaluación de accesibilidad de sistemas biométricos en dispositivos móviles.

-Duración (meses): 6

-Tasa de costes indirectos: 8%

4. Presupuesto total del Proyecto (valores en euros)

14.070,50 euros.

5. Desglose presupuestario

PERSONAL				
Apellido, Nombre	**Categoría**	**Dedicación** $(Hombre\ mes)^a$	**Coste hombre mes(€/mes)**	**Coste total (Euros)**
Blanco Gonzalo, Ramón	Doctor ingeniero	1,2	4.289,54	5.147,45 €
Ludeña Sanchez-Bayuela, Alvaro	Ingeniero	2,8	2.694,39	7.544,29 €
			Total	12.691,74 €

a) 1 hombre mes =131.25 horas. Máximo anual de dedicación de 12 hombres mes (1.575 horas)
Máximo anual para PDI de la universidad Carlos III de Madrid de 8.8 hombres mes (1.155 horas)

Equipos					
Descripción	**Coste (Euro)**	**% Uso dedicado al proyecto**	**Dedicación (meses)**	**Periodo de depreciación (meses)**	$Coste\ imputable^b$
Dispositivo móvil 3T One plus	440,00 €	100	6	36	73,33 €
Dispositivo Tablet Sony Xperia Z	499,00 €	100	6	36	83,17 €
				Total	156,50 €

b) Fórmula cálculo de amortización: $\frac{A}{B} x C x D$

A=Nº meses desde la fecha de facturación en que el equipo es utilizado

B=Periodo de depreciación

C=Coste del equipo

D= % del uso que se dedica al proyecto (habitualmente 100%)

Otros costes directos del proyecto[c]		
Descripción	**Empresa**	**Gasto imputable**
Viajes en coche al CRMF	Propio	180,00 €
	Total	180,00 €

c)Este capítulo de gastos incluye todos los gastos no contemplados en los conceptos anteriores, por ejemplo: fungibles, viajes y dietas, otros, …

6. Resumen de costes

Resumen de costes		
Directos	Personal	12691,74
	Equipos	156,5
	Otros costes directos	180
	Total costes directos	13.028,24 €
Indirectos	Total costes indirectos	1.042,26 €
	Total costes	**14.070,50 €**

El presupuesto total del presente proyecto asciende a la cantidad de 14.070,50 EUROS.

Leganés a 10 de octubre de 2017.

El ingeniero proyectista,

Fdo. Alvaro Ludeña Sanchez-Bayuela

Anexo 1. Documento de aceptación.

	Grupo Universitario de Tecnologías de Identificación Departamento de Tecnología Electrónica
DOCUMENTO DE CONFORMIDAD	

Introducción

Está siendo invitado/a a tomar parte en un proyecto de investigación que tiene como finalidad mejorar el diseño y el rendimiento de sistemas de reconocimiento biométrico de personas. Con este fin, se va a crear una base de datos compuesta por datos que se obtienen de sus parámetros biométricos y/o personales, que será utilizada para llevar a cabo el análisis y la evaluación del rendimiento de dichos sistemas.

Antes de decidir participar en este proyecto, es importante que usted comprenda el motivo y el proceso de recogida de datos y lo que este hecho supone. Por favor, tómese su tiempo para leer la siguiente información y no dude en preguntar a la persona que le va a guiar durante el proceso si encuentra algo que no esté lo suficientemente claro o si necesita más información.

Es importante mencionar que el proceso NO entraña ningún riesgo ni causa daños físicos a la persona.

Detalles del Proceso

El proceso puede contemplar que se tengan que completar varias visitas. En cada visita se obtendrán muestras de sus parámetros biométricos y/o personales, recogidos por dispositivos acondicionados a dicha captura. Un operador le explicará el proceso al inicio y le atenderá durante la evaluación para responder a sus dudas.

En cada una de sus visitas, usted deberá seguir las indicaciones del operador, el cual le indicará cómo será su interacción con el dispositivo de captura, así como la forma de proceder, tanto a la hora de operar con él, como su actitud frente a dicha captura. La finalidad de la evaluación es conseguir muestras de diferentes interacciones, así como de diferentes personas en ese mismo tipo de interacciones, de manera que se pueda evaluar el rendimiento de dichos sistemas.

El tiempo empleado en cada visita es aproximado y dependerá, tanto de su experiencia previa, como de la variedad de las interacciones requeridas. Tómese su tiempo, y siga, lo más fielmente posible las indicaciones del operador.

¿Qué pasará con los datos personales?

Los datos personales recogidos serán incorporados y tratados en la base de datos "BIOMETRIA_GUTI_UC3M" recogida dentro del Fichero "PROYECTOS DE INVESTIGACIÓN" declarado en la AEPD con número de registrado 2140150008. Su finalidad será el análisis del rendimiento de diferentes sistemas de reconocimiento de personas teniendo en cuenta las características de los individuos que pueden influir en distintas tecnologías de reconocimiento, teniendo en cuenta distintos aspectos suyos, tales como edad, género o grado de uso de la tecnología.

Este fichero inscrito en el Registro General de Protección de Datos de la AEPD y cumplirá con lo allí dispuesto en temas de cesiones de los datos, restringiéndose éstas a las especificadas por la ley. En

1 de 2

concreto, los datos de identificación personal (nombre y NIF) serán entregados a la Administración General del Estado para el cumplimiento de la legislación vigente en caso de ser requeridos.

Dichos datos personales serán mantenidos en la base de datos durante un tiempo mínimo de un año. Transcurrido dicho tiempo, si no ha ejercido su derecho a eliminación de los datos, estos serán anonimizados para su uso en posteriores investigaciones. Es decir, los datos que permitan su identificación directa (por ejemplo, nombre, DNI, fotografía facial, etc.) serán eliminados, pasando a ser el resto de datos numerados de forma que se puedan seguir utilizando para estudios estadísticos. En caso de que Vd. ejerza su derecho a eliminación, estos datos serán eliminados completamente al término de la investigación o de dicho plazo de un año.

¿Cómo puedo ejercer mis derechos conforme a la LOPD?

El órgano responsable de ambos ficheros es la Universidad Carlos III de Madrid, y la dirección donde el interesado podrá ejercer los derechos de acceso, rectificación, cancelación y oposición ante el mismo es: **protdatos@listserv.uc3m.es**; todo lo cual se informa en cumplimiento del artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Para ejercer dicho derecho, debe Vd. indicar dicho deseo junto a su nombre completo, DNI y el nombre de la base de datos especificada anteriormente (es decir, BIOMETRIA_GUTI_UC3M).

Consentimiento:

Yo _____, con DNI _____ reconozco haber leído y entendido las condiciones anteriormente redactadas en este escrito y acepto tomar parte en el proceso de adquisición de muestras de reconocimiento de personas.

Fdo:

Fecha:

Anexo 2. Cuestionario de inicio

Cuestionario de inicio

Cuestionario que se realiza en la visita 1 antes de manipular el dispositivo móvil. La finalidad de este cuestionario es obtener resultados estadísticos que nos ayuden a comprender y mejorar los sistemas biométricos para lograr una mayor comodidad y efectividad a la hora de usar dichos sistemas. Todos los cuestionarios son anónimos. Lean las preguntas detenidamente y pregunten cualquier duda que tengan al evaluador. Tomense su tiempo, este cuistionario solo le llevara 2 minutos.

*Obligatorio

1. **Nombre del encuestado** *

_____

2. **1. ¿Es usted...?** *

Marca solo un óvalo.

- ◯ Mujer
- ◯ Hombre

Sección sin título

3. **2. ¿Su edad está comprendida entre?** *

Marca solo un óvalo.

- ◯ 18-30
- ◯ 31-50
- ◯ 51-70
- ◯ +70

4. **3. ¿Cuál es su grado de estudios?** *

Marca solo un óvalo.

- ◯ Sin estudios
- ◯ Graduado escolar
- ◯ Bachillerato
- ◯ Universitarios

5. **4. ¿Tiene algún problema de accesibilidad? En caso afirmativo indicar cual.** *

_____

_____

_____

_____

_____

6. **5. ¿Es usted...?** *
   Marca solo un óvalo.
   - ◯ Zurdo
   - ◯ Diestro

7. **6. ¿Está familiarizado/a con la tecnología en general? En caso afirmativo indique con qué tipo de dispositivos está más familiarizado/a (elija al menos 1).** *
   Marca solo un óvalo.
   - ◯ Ordenadores
   - ◯ Cámaras
   - ◯ Biométricos
   - ◯ Móviles

8. **7. ¿Ha tenido alguna experiencia previa con dispositivos biométricos (por ejemplo, huella dactilar, reconocimiento de voz...)?** *
   Marca solo un óvalo.
   - ◯ Si
   - ◯ No

9. **7.1. En caso afirmativo en la pregunta 7, indique cuál:** *
   _____
   _____
   _____
   _____
   _____

10. **8. ¿Qué preferiría utilizar?** *
    Marca solo un óvalo.
    - ◯ Huella
    - ◯ reconocimiento facial
    - ◯ Voz
    - ◯ Pin
    - ◯ Patrón

11. **9. ¿Utilizaria la biometría para desbloquear su móvil / ordenador? En caso negativo marque 1 o varias** *
    Marca solo un óvalo.
    - ◯ Si
    - ◯ No, por que es lento
    - ◯ No por que es incómodo
    - ◯ No, por que es inseguro
    - ◯ No, por que es dificil
    - ◯ Otro: _____

12. **10. ¿Utilizaría la biometría para realizar pagos, sacar dinero en un cajero, etc.? En caso negativo marque 1 o varias** *

Marca solo un óvalo.

- ◯ Si
- ◯ No, por que es lento
- ◯ No, por que es incómodo
- ◯ No, por que es inseguro
- ◯ No, por que es difícil
- ◯ Otro: _____

13. **11. ¿Utiliza alguna aplicación móvil accesible o las características de accesibilidad (VoiceOver, Talkback)? Indique cuál** *

Marca solo un óvalo.

- ◯ No, por que no la necesito
- ◯ No, por que no las conozco
- ◯ No por que es difícil
- ◯ Si

14. **11.1.En caso afirmativo en la pregunta 12 indique que aplicación/es usa.** *

_____

_____

_____

_____

_____

Con la tecnología de Google Forms

Anexo 3. Cuestionario final

Cuestionario final visita 2

Este cuestionario es la continuación del cuestionario que realizó en la visita 1. El cuestionario es anónimo. Por favor tómese su tiempo para responder, tan solo le llevará 2 minutos. Cualquier pregunta que no vea clara o no se entienda no dude en preguntar al evaluador. Los datos se usarán para realizar un estudio estadístico y así poder mejor las aplicaciones biométricas y lograr una mejor interacción entre los usuarios y las aplicaciones biométricas

*Obligatorio

1. **Nombre el encuestado** *

2. **1. ¿Le ha resultado cómodo utilizar el reconocimiento facial? (0-Muy Incómodo /5-Muy Cómodo)(6-NS/NC)** *
   Marca solo un óvalo.

0	1	2	3	4	5	6
◯	◯	◯	◯	◯	◯	◯

3. **2. Considera que el tiempo por reconocimiento facial ha sido(0-Muy Largo / 5-Muy corto) (6-NS/NC)** *
   Marca solo un óvalo.

0	1	2	3	4	5	6
◯	◯	◯	◯	◯	◯	◯

4. **3. ¿Le ha resultado cómodo utilizar el PIN de 4 dígitos? (0-Muy Incómodo / 5-Muy Cómodo)(6-NS/NC)** *
   Marca solo un óvalo.

0	1	2	3	4	5	6
◯	◯	◯	◯	◯	◯	◯

5. **4. Considera que el tiempo por uso de PIN ha sido (0-Muy Largo / 5-Muy corto)(6-NS/NC)** *
   Marca solo un óvalo.

0	1	2	3	4	5	6
◯	◯	◯	◯	◯	◯	◯

6. **5. ¿Le ha resultado cómodo utilizar el patrón de seguridad? (0-Muy Incómodo / 5-Muy Cómodo) (6-NS/NC)** *
   Marca solo un óvalo.

0	1	2	3	4	5	6
◯	◯	◯	◯	◯	◯	◯

7. **6. Considera que el tiempo por patrón de seguridad ha sido...(0-Muy Largo / 5-Muy corto) (6-NS/NC)** *
   Marca solo un óvalo.

0	1	2	3	4	5	6
◯	◯	◯	◯	◯	◯	◯

8. **7. ¿Le ha resultado cómodo utilizar el reconocimiento de voz? (0-Muy Incómodo /5-Muy Cómodo)(6-NS/NC)** *
   Marca solo un óvalo.

0	1	2	3	4	5	6
◯	◯	◯	◯	◯	◯	◯

9. **8. Considera que el tiempo por reconocimiento de voz ha sido... (0-Muy Largo / 5-Muy corto)(6-NS/NC)** *
   Marca solo un óvalo.

0	1	2	3	4	5	6
◯	◯	◯	◯	◯	◯	◯

10. **9. ¿Le ha resultado cómodo utilizar la huella dactilar? (0-Muy Incómodo/5-Muy Cómodo)(6-NS-NC)** *
    Marca solo un óvalo.

0	1	2	3	4	5	6
◯	◯	◯	◯	◯	◯	◯

11. **10. Considera que el tiempo por huella dactilar ha sido... (0-Muy Largo / 5-Muy corto)(6-NS/NC)** *
    Marca solo un óvalo.

0	1	2	3	4	5	6
◯	◯	◯	◯	◯	◯	◯

12. **11. ¿Considera suficientes las instrucciones recibidas?** *
    Marca solo un óvalo.

- ◯ Si
- ◯ No

13. **12. En general ¿qué preferiría utilizar?** *
Marca solo un óvalo.

- ◯ Huella
- ◯ Reconocimiento facial
- ◯ Reconocimiento por voz
- ◯ Código PIN
- ◯ Patrón de seguridad
- ◯ Ninguno

14. **13. ¿Utilizaría la biometría para desbloquear su móvil / ordenador?** *
Marca solo un óvalo.

- ◯ Si
- ◯ No, por que es lento
- ◯ No, por que es incómodo
- ◯ No, por que es inseguro
- ◯ No, por que es dificil
- ◯ Otro: _____

15. **14. ¿Utilizaría la biometría para realizar pagos, sacar dinero en un cajero, etc.?** *
Marca solo un óvalo.

- ◯ Si
- ◯ No, por que es lento
- ◯ No, por que es incómodo
- ◯ No, por que es inseguro
- ◯ Otro: _____

16. **15. ¿Ha tenido alguna dificultad para completar la evaluación? En caso afirmativo, indique cual:** *
Marca solo un óvalo.

- ◯ Si, por que los dispositivos son incómodos
- ◯ Si, necesité muchos intentos
- ◯ Si, tardé demasiado
- ◯ Si, no es intuitivo ni fácil de usar
- ◯ No he tenido dificultades
- ◯ Otro: _____

Con la tecnología de
Google Forms

Bibliografía

[1] «CRMF Madrid,»

Available: http://www.crmfmadrid.es/crmfmadrid_01/index.htm

[Último acceso: 22 Septiembre 2017].

[2] GUTI, «University Group for Identification Technologies (UC3M),»

Available: http://guti.uc3m.es/

[Último acceso: 22 Septiembre 2017].

[3] ABCTECNOLOGÍA, «MediaTrends,» 8 Noviembre 2016.

Available: http://www.abc.es/tecnologia/moviles/telefonia/abci-espana-pais-mas-smartphones-habitante-mundo-201611081019_noticia.html

[Último acceso: 22 Septiembre 2017].

[4] A. K. Jain, Handbook of Biometrics, Springer, 2007.

[5] M. Rouse, «TechTarget,» 1 Octubre 2008.

Available: http://searchdatacenter.techtarget.com/es/definicion/Biometria

[Último acceso: 22 Septiembre 2017].

[6] A. Bertillon, Alphonse Bertillon's Instructions For Taking Descriptions For The Identification Of Criminals And Others, By Means Of Anthropometric Indications, Kessinger Publishing, 2010.

[7] F. Galton, Inquiries into Human Faculty and Its Development, Macmillan & Co., 1883.

[8] G. E. D. Parra, «Ingeniería de Sistemas-Biometría,»

Available:https://upload.wikimedia.org/wikipedia/commons/c/ce/Articulo_gerson_delgado_congsistel.pdf

[Último acceso: 22 Septiembre 2017].

[9] P. Jonathon Philips, H. Wechsler, J. Huang y P. Rauss, «The FERET database and evaluation procedure for face-recognition algorithms,» 1998.

[10] iSecureBios, 19 Octubre 2010.

Available: http://biometria-isecurebios.blogspot.com.es/2010/10/diferencia-entre-identificacion-y.html

[Último acceso: 22 Septiembre 2017].

[11] A. H. Briones, «UNAM-Facultad de Ingeniería Biométrica Informática,» 2000.

Available:http://redyseguridad.fi-p.unam.mx/proyectos/biometria/basesteoricas/arquitectura.html

[Último acceso: 22 Septiembre 2017].

[12] R. Blanco Gonzalo, Usability in biometric recognition systems, 2016.

[13] A. H. Briones, «UNAM-Facultad de Ingeniería Biométrica Informática,» 2000.

Available:http://redyseguridad.fi-p.unam.mx/proyectos/biometria/basesteoricas/moduloinscripcion.html

[Último acceso: 22 Septiembre 2017].

[14] «International Organization for Standardization, ´ISO 9241-11:1998´ Ergonomic requirements for office work with visual display terminals(VDTs) — Part 11: Guidance on usability,» 1998.

Available: https://www.iso.org/obp/ui/#iso:std:iso:9241:-11:ed-1:v1:en

[Último acceso: 22 Septimbre 2017].

[15] «International Organization for Standardization, ´ISO 26800:2011´, Ergonomics-General approach, principles and concepts,» 2011.

Available: https://www.iso.org/obp/ui/#iso:std:iso:26800:ed-1:v1:en

[Último acceso: 22 Septiembre 2017].

[16] « CEN, CENELEC, ETSI. EN 301 549. v1.1.1. accessibility requirements suitable for public procurement of ICT products and services in europe,» Abril 2015.

Available:http://www.etsi.org/deliver/etsi_en/301500_301599/301549/01.01.02_60/en_301549v010102p.pdf

[Último acceso: 22 Septiembre 2017].

[17] «International Organization for Standardization, ´ISO/IEC 19795-2:2007´, Information Technology - Biometric Performance Testing and Reporting - Part 2: Testing methodologies for technology and scenario evaluation,»

Available: https://www.iso.org/obp/ui/#iso:std:iso-iec:19795:-2:ed-1:v1:en
[Último acceso: 22 Septiembre 2017].

[18] B. Fernandez-Saavedra, R. Alonso-Moreno, J. Uriarte-Antonio y R. Sanchez-Reillo, «Evaluation methodology for analyzing usability factors in biometrics,» 2010.

[19] «International Organization for Standardization-ISO/IEC 19795-1:2006 "Biometric performance testing and reporting — Part 1: Principles and framework",»

[20] «Agnitio 360 voice ID,» 2016. [En línea].

Available:http://www.agnitio-corp.com/products/commercial/voice-recognition-software

[Último acceso: 22 Septiembre 2017].

[21] P. V. y M. J. , «Rapid object detection using a boosted cascade of simple features,» 2001.

[22] D. Loewe, Distinctive Image Features from Scale-Invariant Keypoints, vol. 60, 2004, pp. 91-110.

[23] J. L. A. Aguilera, Evaluación de accesibilidad en aplicación móvil de pagos con biometría, 2015.

[24] A. H. Briones, «UNAM-Facultd de Ingeniería Biométrica Informática,» 2000. Available:http://redyseguridad.fi-p.unam.mx/proyectos/biometria/basesteoricas/moduloidentificacion.html

[Último acceso: 22 Septiembre 2017].

[25] O. C. Montoto, «usableaccesible,» 2012 Marzo 15.

Available: https://olgacarreras.blogspot.com.es/

[Último acceso: 22 Septiembre 2017].